HP StorageWorks
Reference Information Storage System
Administrator Guide

Product Version: 1.0

First Edition (April 2004)

Part Number: AA–RV1PA–TE

HP StorageWorks Reference Information Storage System Administrator Guide
First Edition (April 2004)
Part Number: AA–RV1PA–TE

Contents

Chapter 1: Key Concepts

Chapter 2: Persist Control Center

Chapter 3: Persist Account Manager

CHAPTER 1

Key Concepts

This chapter provides background on the key concepts involving the HP StorageWorks Reference Information Storage System (RISS).

It contains the following topics:

RISS – Purpose and Tools

The **HP StorageWorks Reference Information Storage System** (RISS) comprises **hosts** (hardware components and their operating systems) and **services** (software application processes) that together provide the following main functions:

- Automatic, active **data archiving** (email and specific types of documents) in a secure, fault-tolerant manner that can help customers meet their regulatory requirements
- Interactive **data querying** to search for and retrieve archived data according to various criteria. Access to archived data is controlled: query users can retrieve data only from the **repositories** to which they have access.

The kinds of data that can be archived and queried depend on how RISS (called the "system" throughout this guide) is configured. At a minimum, email messages are supported on all systems. References to messages in PCC views, and in this guide, include documents when the system supports the archiving of documents.

In addition to these principal functions, RISS provides the following trouble-shooting and administrative tools:

- The **Persist Control Center** (**PCC**), used to monitor and troubleshoot system status and performance.
- The **Persist Account Manager** (**PAM**), used to manage user accounts.

See also

- The *HP StorageWorks Reference Information Storage System User Guide,* for information on querying data.
- Chapter 2, Persist Control Center.
- Chapter 3, Persist Account Manager.

Monitoring and Reporting Tool

Persist Control Center

The Persist Control Center (**PCC**) monitors the system and reports on its health and activity. PCC provides reports on all of the following:

- system health (status)
- system performance
- smart cell states

Hosts in the system (and their services) are organized into groups of the same type, called **host groups**. You can, for example, look at all hosts of type smart cell, by displaying the status of the host group SmartCells.

The expression "**Persist Control Center**" refers to both the behind-the-scenes monitoring functions and the user interface that reports on their findings. In both of these roles, the system uses software provided by Nagios, `www.nagios.org`. (The PCC is part of the system it monitors, so it monitors itself, as well – see *Nagios Info*, on page 2-39, and *Nagios Stats*, on page 2-42.)

Monitoring and Reporting Methods

System monitoring is reported both online, with a web-based (HTML) user interface, and offline, by email to selected contacts. Email reporting provides a subset of the information provided online.

Hosts and services are monitored by polling. You schedule the polling intervals for services, but host polling is purposely kept to a minimum. Depending on the polling interval, there is more or less delay between occurrences on the system and the reporting of those occurences in the PCC interface. In general, a host is polled only at system startup and after one or more service checks indicate a potential host problem. As long as the services appear to be functioning correctly (OK), the host is assumed to be healthy (UP). You can selectively enable or disable polling of hosts and services.

If monitoring indicates that a host is not functioning correctly (DOWN), then none of its services are available (they can be reported as having any status except OK). If a service is reported as having CRITICAL status, but the host is UP, it is likely that the service needs to be restarted.

Status and State

Various PCC views show the current life cycle **states** of smart cells or the **status values** of particular hosts or services. A status value measures relative health. It can be associated with a **status condition** that conveys a measure of confidence in the reported value. This section defines the possible life cycle states, status values, and status conditions.

For example, the health of a smart cell in the life cycle state DEAD can be reported with host status value DOWN. If the host status value has been checked the required number of times, the status condition is reported as HARD (otherwise it is SOFT).

PCC views (see *User Interface Components*, on page 2-2) often use the terms "status" and "state" loosely, and interchangeably when referring to hosts and services. They always use "state" when referring to smart cell life cycle states, but they use both "status" and "state" when reporting on the health of a smart cell, regarding it as a host like any other. PCC views also refer to a status condition as a "state" or "state type."

Status of system components is color coded: **green** indicates normal operation; **red** indicates the component has stopped or failed; **yellow** indicates a warning. See *Host and Service Status Value Definitions*, on page 1-6.

Smart Cell Life Cycle State Definitions

The following table defines the possible smart cell life cycle states.

Table 1-1: Smart Cell Life Cycle State Definitions

Life-cycle State	Definition	Importance
DISCOVERY	The metaserver and the smart cell are determining the start state for the cell (state following DISCOVERY), based on the expected states of the cell and its mirror smart cell. The cell is not available for document storage, search, or retrieval.	maintenance (startup only)

Table 1-1: Smart Cell Life Cycle State Definitions (Continued)

Life-cycle State	Definition	Importance
ASSIGNED	The cell has been assigned to a domain. It is available for document storage, search, and retrieval. If backup is enabled, cell data can be backed up.	normal
COMPLETE_ PROCESSING	Data indexing is being completed. The cell is full. It is available for document search and retrieval, but not for storage. If backup is enabled, cell data can be backed up.	maintenance
BACKING_UP	The cell is available for document search and retrieval. If backup is enabled, cell is backing up all of its indexes and any new data that has not yet been backed up.	maintenance
SYNC_WAIT	The cell is available for document search and retrieval.	maintenance
CLOSED	The cell is full. It is available for document search and retrieval, but not for storage. If backup is enabled, all cell data has been backed up before the cell enters this state.	normal
RESET	The cell is being recycled. Stored documents and corresponding management data, such as document indexes, are destroyed during recycling. A system administrator has determined that the existing cell data is no longer needed. The RESET state is only set manually. The cell is not affiliated with any domain, so it is not available for document storage, search, or retrieval.	maintenance
FREE	The cell can become ASSIGNED or become a target for data restoration. It is not affiliated with any domain, so it is not available for document storage, search, or retrieval.	normal
RESTORE	The cell is a target for data restoration from another smart cell. It is not available for document storage, search, or retrieval.	maintenance

Table 1-1: Smart Cell Life Cycle State Definitions (Continued)

Life-cycle State	Definition	Importance
DEAD	The cell requires attention. It is not available for document storage, search, or retrieval. If backup is enabled, some or all cell data may *not* have been backed up; if so, it will *never* be backed up.	failure
SUSPENDED	Either of the following is true: • The cell or its mirror cell has one or more failed processes. In this case both are SUSPENDED. • The mirror cell is DEAD. *Note:* If the Application Health service for the cell is OK, then it is (only) the mirror cell that has failed. (You can use the Service Detail view to check this service.) The cell is not available for storage. It is available for document search and retrieval (unless a failed process has disabled the search engine). If backup is enabled, the cell is backing up any new data that has not yet been backed up.	failure

Host and Service Status Value Definitions

The following tables define the possible host and service status values and the associated color coding used in some PCC views. The normal values are UP (host) and OK (service), indicated by shading.

Table 1-2: Host Status Value Definitions

Status	Color	Description
PENDING	Gray	The host has not yet been checked for its status. When the PCC first starts monitoring the services associated with a host, the host status value is set to PENDING.
UP	Green	The host is running. It responds to status checks.
DOWN	Red	The host is not running and does not respond to status checks.
UNREACHABLE	Brown	The parent cloud router of the UNREACHABLE smart cell or HTTP portal is DOWN.

Table 1-3: Service Status Value Definitions

Status		Description
PENDING	Gray	The service has not been checked for its status since the startup of PCC monitoring.
OK	Green	The service is functioning normally.
WARNING	Yellow	The service may have a problem.
UNKNOWN	Orange	The status of the service cannot be determined.
CRITICAL	Red	The service is not functioning correctly. Data storage and/or search/retrieval are adversely affected.

See Also

- *Monitoring and Reporting Tool*, on page 1-3, for information on how status values are determined.

Hard and Soft Status Condition Definitions

A host or service status value is reported in alerts and other events as having a HARD or SOFT status condition (also referred to in monitoring views as the "state type"). See, for example, the following views:

- *Alert Histogram*, on page 2-60
- *Alert History*, on page 2-64
- *Alert Summary*, on page 2-66
- *Event Log*, on page 2-74

A SOFT status condition indicates that the status value has not yet been confirmed; a HARD condition has been confirmed. Confirmation is required only for problem status values, not for the normal operation values UP, for hosts, and OK, for services. A normal status value always has a HARD status condition.

When a host or service problem is detected, the PCC rechecks the problem a certain number of times. During this trial period, the status condition is considered SOFT. After rechecking the required number of times with the same result, the status condition is considered HARD.

The required number of checks for a given host or service is displayed in the View Config view (Hosts or Services Object Type, respectively). See *View Config*, on page 2-94.

CHAPTER 2

Persist Control Center

This chapter describes the Persist Control Center (PCC), the tool you use to monitor and troubleshoot RISS.

It contains the following topics:

See Also

- *Monitoring and Reporting Tool*, page 1-3, for definitions and explanations of the key concepts involving the PCC and monitoring of system status.

Tour of the PCC User Interface

User Interface Components

The PCC graphical user interface comprises a set of cross-linked HTML pages. At the right of each page is a monitoring, reporting, or tools **view**; at the left is a menu (referred to here as the **left menu**), which provides direct access to some views. Many views also provide links to other, related views.

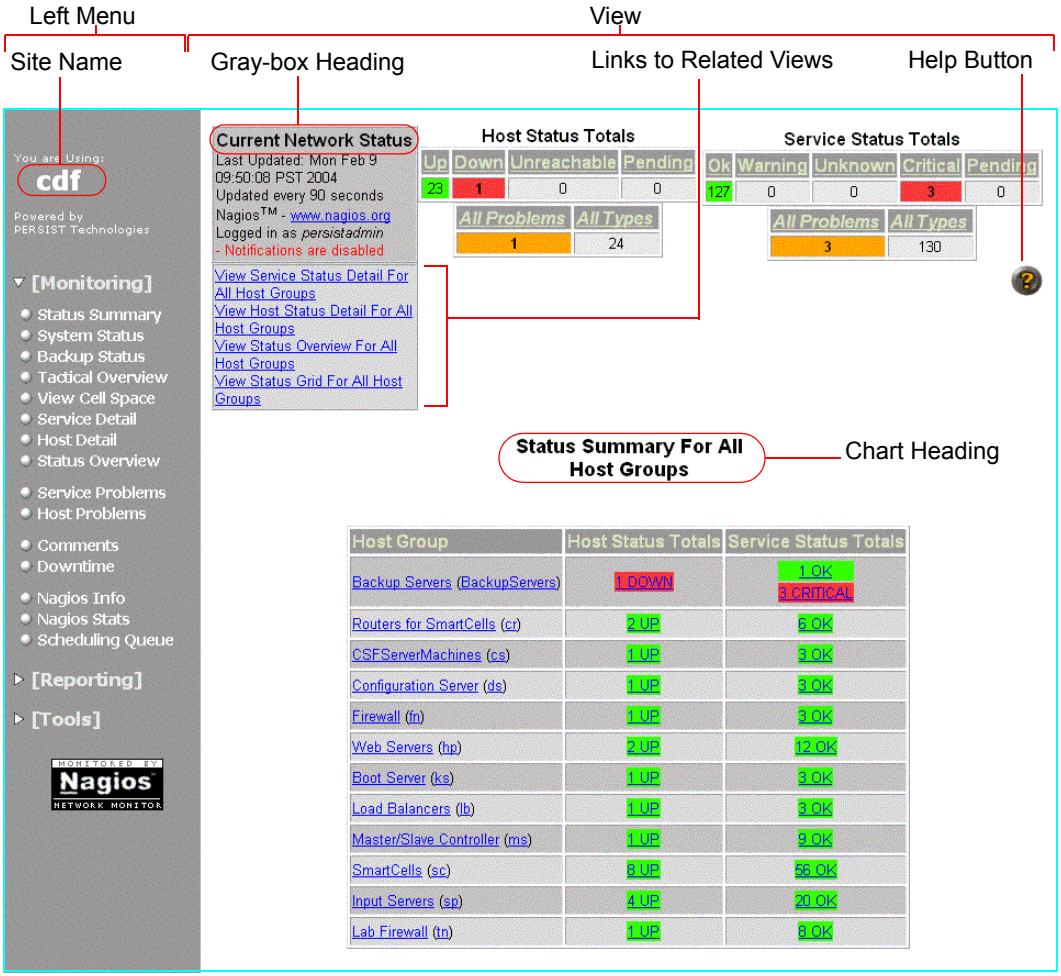


Figure 2-1: Persist Control Center User Interface

Views for Common Tasks

The following table lists the views for common system administration tasks. These are some of the views you will become most familiar with.

Table 2-1: Views to Use for Common Tasks

To do this . . .	Use this view . . .
Check system health.	*Status Summary*, page 2-11 and the frst item in the PCC left menu
	If everything is green, the system is healthy. If anything is red, click it to zoom in and examine the problem.
Check system performance.	*System Status*, page 2-14 and the second item in the PCC left menu
	High store and indexing rates are good. Low query times are good. You can zoom in on an hourly period by clicking the period in the Last 24 Hours bar.
Check smart cell health/performance.	*Smart Cell Groups for Domain*, page 2-112
Check status of backups.	*Backup Status*, page 2-18
Clone a smart cell (copy the data).	*SmartCell Cloning*, page 2-91
Monitor system alerts.	*Alert History*, page 2-64
Configure periodic email reports of system status and performance.	*EmailReporter*, page 2-44
Enable automatic email notifications for important system events, such as host/service problems and recoveries.	*Nagios Info*, page 2-39
Communicate problems, instructions, and so on as comments (and read co-workers' comments).	*Comments*, page 2-36
Start, stop, and restart servers on the system.	*Application Manager*, page 2-76
Monitor, start, and stop replication for domains.	*Replication*, page 2-78

Table 2-1: Views to Use for Common Tasks (Continued)

To do this . . .	Use this view . . .
Display status information about the email mining servers.	*Email Mining*, page 2-81

Monitoring and Reporting Views

The following tables show PCC monitoring, reporting, and tools views (not all views are listed), organized by general purpose or point of view. The most commonly used views are Status Summary, System Status, Smart Cell Groups for Domain, EmailReporter, Alert History, Application Manager, Replication, and Email Mining, as indicated by the shaded cells.

Table 2-2: PCC Monitoring Views

	General Views	Detailed Views	Problem Views	
System Views	Status Summary	Host Detail	Host Problems	**Host Views**
	Tactical Overview	System Status		
	Status Overview	Smart Cell Groups for Domain		
	View Cell Space	Service Detail	Service Problems	**Service Views**
	Backup Status			
Management Views	Comments	Scheduling Queue		
	Downtime			
Nagios Views	Nagios Info	Nagios Stats		

Table 2-3: PCC Reporting Views

Reports	Alerts	Logs
EmailReporter	Alert Histogram	Notifications
Trends	Alert History	Event Log
Availability	Alert Summary	

Table 2-4: PCC Tools Views

Status	Actions
Application Manager	SmartCell Cloning
Replication	Update PCC
Email Mining	
User Manager	
Software Versions	
View Config	

Left Menu Views

The left menu provides quick access to many PCC views. The following tables summarize the views that are accessible from the three sections of the left menu: Monitoring, Reporting, and Tools. The most commonly used views are Status Summary, System Status, EmailReporter, and Alert History, as indicated by the shaded cells.

Table 2-5: Monitoring Views Accessible From the Left Menu

Left Menu Item	Description	See Page
Status Summary	High-level view of system health, showing for each host group how many hosts and services have each status value. Lets you see the status of each host group without detail.	2-11

Table 2-5: Monitoring Views Accessible From the Left Menu (Continued)

Left Menu Item	Description	See Page
System Status	A summary of system domains, smart cells, exceptions, and current software versions, along with graphs of system performance. Gives you an overview of system capacity and performance.	2-14
Backup Status (Optional feature)	State and status information about the backup server and services. Lets you see what backup services are enabled, the results of the last backup, and any alerts or warnings.	2-18
Tactical Overview	High-level view of system health and monitoring, showing how many hosts and services have each status value and which monitoring features are enabled. Lets you quickly see overall system status and also set monitoring features.	2-21
View Cell Space	• Names of important hosts organized by host group. • Life cycle states and health of smart cells in each domain. Lets you determine the status of the data archiving system.	2-24
Service Detail	The status of services running on each host, organized by host groups. Lets you examine details of particular services.	2-26
Host Detail	Status information for each host in the system. Lets you examine details of particular hosts.	2-30
Status Overview	• Status of the hosts in each host group. • High-level view of the status of the services on each host. Lets you see the status of each host in all host groups, including the status of all services on the host.	2-32
Service Problems	Status information for each service that has a problem. A subset of the Service Detail view. Lets you examine details of problem services.	2-34

Table 2-5: Monitoring Views Accessible From the Left Menu (Continued)

Left Menu Item	Description	See Page
Host Problems	Status information for each host that has a problem. A subset of the Host Detail view. Lets you examine details of problem hosts.	2-35
Comments	System administrators' comments. Lets you view and add comments to communicate with other system administrators.	2-36
Downtime	Scheduled downtime for hosts and services. Lets you view and schedule host and service downtimes; disables notifications during downtimes.	2-37
Nagios Info	Information about the PCC host and service monitor. Lets you control monitoring and check monitoring status. This is also where you enable and disable notifications globally, for all hosts and services.	2-39
Nagios Stats	Information on the performance of PCC host and service monitoring. Lets you check monitoring performance.	2-42
Scheduling Queue	Schedule of service checks for each host in the system. Lets you view and schedule service checks.	2-43

Table 2-6: Reporting Views Accessible From the Left Menu

Left Menu Item	Description	See Page
EmailReporter	Lets you configure summary monitoring reports to be sent periodically to email recipients you choose.	2-44
Trends	Lets you create reports on the status of individual hosts or services over given time periods.	2-51
Availability	Lets you create reports on the availability of individual hosts, services, or host groups over given time periods.	2-55
Alert Histogram	Lets you create reports with simple graphs for different time periods showing, for individual hosts or services, the number of events for each status value.	2-60

Table 2-6: Reporting Views Accessible From the Left Menu (Continued)

Left Menu Item	Description	See Page
Alert History	Lists the most recently logged alerts.	2-64
Alert Summary	Lets you create reports summarizing different types of alerts over different periods.	2-66
Notifications	Lists the host and service notifications of different types that have been sent to the system contact (persistadmin). Lets you see what notifications were sent, when.	2-71
Event Log	Lists the most recently logged events.	2-74

Table 2-7: Tools Views Accessible From the Left Menu

Left Menu Item	Description	See Page
Application Manager	Lets you start, stop, or restart one or more servers on the system.	2-76
Replication	Lets you monitor and start or stop replication for one or more domains.	2-78
Email Mining	Displays status information for the mining system on each domain, along with graphs of the message store rate.	2-81
User Manager	Lets you configure Dynamic Account Synchronization to automatically create and update RISS users with information obtained from LDAP servers.	2-83
SmartCell Cloning	Lets you clone a smart cell (copy its data) in order to give it a new, viable mirror cell.	2-91
Update PCC	Updates the PCC to use the latest system configuration.	2-93
Software Versions	Lists the software versions of hosts in the system.	2-94
View Config	Displays overviews of the entire system configuration from various points of view based on object types (hosts, services, contacts, commands, and so on). Lets you examine system parameters as defined during system configuration.	2-94

See Also

- *User Interface Components*, page 2-2, for more information on the left menu.
- *Smart Cell Groups for Domain*, page 2-112, for information on a commonly used view that is inaccessible from the left menu. It provides detailed information on the smart cells in a domain.

User Interface Orientation Tips

As you navigate through PCC views, you will notice that a view is often associated with several names or brief descriptions. Paying attention to the different ways a view is characterized can help you orient yourself:

- *Link text* – A navigation link leading to a view is often the most specific description of the view.

  For example, the link View Status Detail For This Host displays the Host Detail view for a specific host; the link View Host Status Detail For All Hosts displays the Host Detail view for all hosts.

- *Gray-box heading* – Some views have a gray box in the upper left corner that contains information about the latest update of the view and the update frequency (see *User Interface Components*, page 2-2, for an illustration). In addition, the heading in this box sometimes provides an additional characterization of the view contents.

  For example, the gray-box heading for the Nagios Stats view is Performance Information, indicating that the view shows the performance of the Nagios monitoring process.

- *Filter description* – Information that is a subset of information obtained by filtering another view is sometimes indicated by a gray box entitled Display Filters. The box describes the filtering used.

  For example, the Service Problems view provides a subset of the information in the Service Detail view. The Display Filters box indicates that the Service Status Types shown are All Problems.

- *Chart heading* – Some views have several separate charts. The heading of the most prominent chart often reflects the main purpose of the view (see *User Interface Components*, page 2-2, for an illustration).

For example, when the Service Detail view shows information about a single host, the most prominent chart in the view is entitled Service Status Details For Host <*hostname*>.

- *HTML name* – Each PCC view has an HTML name that describes it. A view normally appears in your browser as an HTML frame alongside the left menu, which is another frame. You usually see the HTML name of a view in one of the following circumstances:
  - You print only the view, not the left menu also. Depending on your browser and how it is configured, the HTML name can appear in the printed page header.

    For example, if you print the frame of the Event Log view, the printed page header may be Nagios Log File.
  - You open the view address (URL) in a browser window by itself, without any frames (so, without the left menu). The browser window title then shows the HTML name of the view.[1]

    For example, if you open the left menu item (link) Event Log in a separate window, the window title is Nagios Log File.

See Also

- *Updating and Printing Views*, page 2-117, for information on how to print a view without also printing the left menu.

1. You can open a link in a separate window by right-clicking the link and choosing the shortcut menu item Open In New Window (Microsoft Internet Explorer 6) or Open Link In New Window (Netscape Navigator 7).

PCC Views, Detailed Descriptions

This section describes PCC views in detail.

Status Summary

The Status Summary view provides a high-level look at the system health. Depending on how it is accessed, this view can display information on a single host group or all host groups. It lets you quickly see the overall status of each host group, as described in the table below.

Note: The charts Host Status Totals and Service Status Totals described here are also used by other views. They always refer to the set of hosts and services targeted by the view. For example, if a view describes a single host group, then these charts show only the hosts and services for that host group.

Table 2-8: Status Summary View Features

Feature	Description
Host Status Totals	The number of hosts • with each status value (Up, Down, Unreachable, and Pending) • with a problem (Down, Unreachable, or Pending) • in the system (All Types)
	Click a status column heading, such as Down, to display the Status Overview view filtered to show only the hosts with that status. See *Status Overview*, page 2-32.
Service Status Totals	The number of services • with each service status value (Ok, Warning, Unknown, Critical, and Pending) • with a problem (Warning, Unknown, Critical, or Pending) • in the system (All Types)
	Click a status column heading, such as Critical, to display the Service Detail view filtered to show only the services with that status. See *Service Detail*, page 2-26.

Table 2-8: Status Summary View Features (Continued)

Feature	Description
Status Summary For . . . Host Group . . .	For each target host group, the number of hosts and services that have each status value.
	Click a Host Group name, such as SmartCells, to display the Status Overview view for that host group. See *Status Overview*, page 2-32.
	Click the parenthetical abbreviation of a host group name, such as (sc), to display the Hostgroup Information view for that host group. See *Hostgroup Information*, page 2-100.
	Click the Host Status Totals column entry for a host group and status value, such as 2 DOWN, to display the Service Status Details view filtered for that host group and host status. See *Service Detail*, page 2-26.
	Click the Service Status Totals column entry for a host group and status value, such as 1 CRITICAL, to display the Service Status Details view filtered for that host group and service status. See *Service Detail*, page 2-26.

See Also

- *Host and Service Status Value Definitions*, page 1-6, for individual status value definitions.

Related Views

- The Status Summary view is a subset of the Status Overview view – see *Status Overview*, page 2-32. The Status Summary view only provides the number of hosts having each status value; the Status Overview view provides the status value of each host. Use the Status Summary for a concise summary of all system health.

Table 2-9: Links **To** the Status Summary View

Origin	Link
left menu	Status Summary
Status Overview, page 2-32	View Status Summary . . .
Host Detail, page 2-30	View Status Summary . . .

Table 2-9: Links **To** the Status Summary View (Continued)

Origin	Link
Host Problems, page 2-35	View Status Summary . . .
Service Detail, page 2-26	View Host Status Summary . . .
Status Grid, page 2-108	View Status Summary . . .

Table 2-10: Links **From** the Status Summary View

Destination	Link
Service Detail, page 2-26	View Service Status Detail . . .
Host Detail, page 2-30	View Host Status Detail . . .
Status Overview, page 2-32	View Status Overview . . .
Status Grid, page 2-108	View Status Grid . . .
Hostgroup Information, page 2-100	host group abbreviation, in parentheses – example: (sc)

System Status

The System Status view provides graphical performance and resource information, as described in the following table.

Table 2-11: System Status View Features

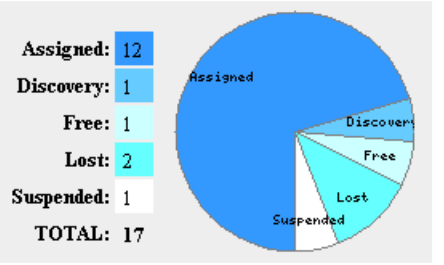
Feature	Description
SmartCell Domain Information	• Names and status of the domains in the system • Total number of messages currently stored in all domains • Total number of messages that could not be parsed (interpreted) or routed in all domains Messages with malformed message structure (MIME) or unsupported character sets cannot be parsed. They are placed in the catch-all repository along with messages that fail to be routed. Click a domain link to display the Smart Cell Groups for Domain view, showing the performance of the smart cell groups for that domain over the last 24 hours. See *Smart Cell Groups for Domain*, page 2-112.
SmartCell Allocation	The number of smart cells in each life cycle state. Lost, when shown, is a pseudostate indicating smart cells whose current life cycle state cannot be determined. Example: 

Table 2-11: System Status View Features (Continued)

Feature	Description
Exceptions	The number of diagnostic messages that were logged for each host group. Support personnel use these messages to diagnose errors reported in the System Status view. Example: Smtp (2) means two exceptions are logged for the Smtp host group.
	Click a link to view the most recent exceptions for the corresponding host group (or All host groups). For example, click Smartcell to display smart cell exceptions. See *Exceptions Stack-trace*, page 2-102. The current event log for the selected host group is filtered to show only exceptions. Any exceptions older than those shown were pruned from the log when it filled up.
Software Versions	Version identifiers for the following installed software groups: • Linux core – third-party software on Linux servers • Windows core – third-party software on the email mining server • Software – HP-developed Java packages • Installer – software on the Kickstart server that installs software on other servers

Table 2-11: System Status View Features (Continued)

Feature	Description
Graph Information	• Other graphs – a link to custom performance graphs of selectable components • 24-hour time bar – selectable time periods for the graph that is displayed at the bottom of the window. You can select the Last 24 Hours or hourly periods expressed in 24-hour (military) format. The selected period has a gray background. (All times are in the time zone where the system is installed.) • Select box – type of data that is displayed in the graph at the bottom of the window. – Appliance Rates shows the store rate (messages stored per second), index rate (messages indexed per second) and indexer latency growth (the store rate minus the index rate) over the selected time period. – Saved Queries shows the average wait time (after the query is submitted until processing starts) and completion time (after processing starts until all results are retrieved) of saved queries. – Unsaved Queries shows the average wait time (after the query is submitted until processing starts), first-page time (after the query is submitted until the first page is displayed), and completion time (after processing starts until the first batch, 500 or less, of results is retrieved) of unsaved queries. • graph – a line graph showing the selected performance data for the selected time period. In a properly operating system, indexer latency growth is zero on average over time: zero means that stored data is being indexed as fast as new data is being stored. A positive value means indexing is slower than storage. Even a small positive value that is maintained over several days means that indexing is falling further and further behind storage. Negative values generally indicate indexing is catching up on a backlog of documents: more stored messages are being indexed than new messages are being stored.
	Click another time period in the 24-hour time bar to update the graph accordingly. For example, select 16 to display store and index rates from 16:00 to 17:00, which is 4:00 pm to 5:00 pm.
	Click the arrow in the Select box to select another data type and update the graph accordingly.
	Click Other Graphs to select and view detailed graphs of system and component performance. You select the component, the metric, and the time period. For example, you can choose to display the minimum, maximum, and average performance of the TSC-NAT machine from 5:00 pm to 6:00 pm on Jan. 26, 2003.

Related Views

- *EmailReporter*, page 2-44, lets you configure a periodic email report similar to the System Status view information.
- *Smart Cell Groups for Domain*, page 2-112, provides Store/Index/Indexer Latency graphs for individual smart cell groups.
- The following views report on the performance of the monitoring system:
  - *Nagios Stats*, page 2-42
  - *Hostgroup Information*, page 2-100
  - *Tactical Overview*, page 2-21

Table 2-12: Links **To** the System Status View

Origin	Link
left menu	System Status
Smart Cell Groups for Domain, page 2-112	Return to Summary
Exceptions Stack-trace, page 2-102	Return to Summary
Other Graphs view – see Other Graphs feature, *System Status View Features*, page 2-14	Return to Summary

Table 2-13: Links **From** the System Status View

Destination	Link
Smart Cell Groups for Domain, page 2-112	domain name (See SmartCell Domain Information.)
Exceptions Stack-trace, page 2-102	host group (See Exceptions.)
Other Graphs view	Other Graphs

Backup Status

The Backup Status view is accessible from the Backup Status left menu item. It provides information on the status of backup servers, signature backups, and data backups. This view is available if your system is configured with the backup feature.

Backup Feature

The backup feature lets you back up all archived messages/documents and digital signatures to write-once-read-many times (WORM) media, including optical media. The feature provides:

- an additional level of data reliability, for the exceptional case where all smart cells in a group fail simultaneously
- disaster recovery of system data

With the backup feature installed, RISS includes an on-site internal backup server. Depending on the configuration, the system may also have an external backup server, located off site but connected to the rest of the system with a virtual private network.

The backup daemon copies data in batches from RISS smart cells once every hour or so.

Compared to message and document backup, signature backup saves space (and is quicker). Signature backup lets you meet compliance requirements for determining if any archived documents have been corrupted. It does *not* back up the messages or documents. If the system configuration provides signature backup duplication, a second backup copy of each signature is created. The two backup copies are produced by primary and duplicate signature backup services.

Tivoli Storage Manager lets you control RISS backup operations. The Backup Status view provides direct access to a Tivoli Server Administration web client.

Backup Status View Features

The Backup Status view is divided into three tabbed panels: Overview, Signatures, and Data Backup. The following tables describe the Backup Status view features.

Table 2-14: Overview Panel Features, Backup Status View

Feature	Description
Backup Status	For each backup server: • General status of the backup server and each of its services. A check icon () indicates normal operation; an X icon () or ! icon () indicates a problem or inactive service. • Remote Administration – Click the Tivoli Console button to access the Tivoli Server Administration web client, providing remote access to the Tivoli servers used for backup. • Summary of active group backup status • For each backup library on the server, the number of volumes and free volumes in the library. A backup library is a collection of backup volumes.
Alerts & Warnings	For each backup server, alerts and warnings currently in effect.

Table 2-15: Signatures Panel Features, Backup Status View

Feature	Description
Signatures backed up	The proportion of signatures that have been backed up, expressed as a percentage and as a ratio of the total number of signatures

Table 2-15: Signatures Panel Features, Backup Status View (Continued)

Feature	Description
Primary Signature Server	Status of the primary signature backup services: • Server Name – Server (Internal or External) where the primary signature backup services run • Library – Name of the library for primary signature backups • Last Backup – How long ago the last primary signature backup occurred • Space Occupied – Number of megabytes of storage used for primary backup of signatures • Volumes – Names of primary signature backup volumes, and how full they are (percentage)
Duplicate Signature Server	Same as Primary Signature Server, with "duplicate" instead of "primary.

Table 2-16: Data Backup Features, Backup Status View

Feature	Description
Library	Name of the library for data backups. A backup library is a collection of backup volumes.
Server Name	Server (Internal or External) where the data backup services run
Files backed up	• The proportion of files that have been backed up, expressed as a percentage and as a ratio of the total number of files • Graph of the percentage of data files backed up over the last 24 hours.

Table 2-16: Data Backup Features, Backup Status View (Continued)

Feature	Description
Active Groups	For each group (pair) of smart cells that are active (*not* closed or suspended): • Domain name and IP address of the smart cell used for backup (usually the secondary smart cell) • Unique smart cell group identification number • Percentage and number of the data files, and the total number of files • Time since last backup cycle – How long ago the last data backup occurred • Group/Backup Daemon Status – State of the smart cell being backed up, and status of the backup daemon (process) • Space Occupied – Number of megabytes of storage used to back up data • Volumes – Names of backup volumes, and how full they are (percentage)
Inactive Groups	Same information as Active Groups, but for inactive groups (closed or suspended smart cells)

See Also

- Tivoli/IBM web site: http://www-3.ibm.com/software/tivoli/.
- *Smart Cell Life Cycle State Definitions*, page 1-4.

Table 2-17: Links **To** the Backup Status View

Origin	Link
left menu	Backup Status

Links from the Backup Status view: none.

Tactical Overview

The Tactical Overview view provides a high-level view of system status (health) and monitoring services. It shows you how many hosts and services have each status value and how many problems are acknowledged and

unacknowledged (unhandled). You can investigate these problems further using other views. This view also lets you enable or disable individual monitoring features.

The following table describes the Tactical Overview view features.

Table 2-18: Tactical Overview View Features

Feature	Description
Monitoring Performance	The current performance of monitoring processes: • Check Execution Time – Minimum, maximum and average times to execute a monitoring check • Check Latency – Minimum, maximum and average durations between the time a monitoring check was scheduled and the time it was executed • # Active Checks – How many services are monitored • # Passive Checks – Currently *not used* (all checks are active)
Network Health	Color-coded indication of the average health of all hosts and services. Green indicates normal operation; red indicates one or more components have stopped or failed; yellow indicates potential problems (warning). See *Host and Service Status Value Definitions*, page 1-6, for more information.
Hosts	Number of hosts with each host status value Click the number of hosts with a given status value, for example 2 DOWN, to display a filtered Service Status Details view for all services running on those hosts – see *Service Detail*, page 2-26. The hosts with problem status values are divided into those with acknowledged problems and the rest (unhandled). Click the appropriate link to show details of those hosts: • <#> Unhandled Problems • <#> Acknowledged Either link displays a filtered Service Status Details view for the appropriate hosts – see *Service Detail*, page 2-26. See *Example: Acknowledging a Problem*, page 2-115, for information on acknowledging a problem.

Table 2-18: Tactical Overview View Features (Continued)

Feature	Description
Services	Number of services with each service status value
	Click the number of services with a given status value, for example 3 CRITICAL, to display the Service Status Details view for those services – see *Service Detail*, page 2-26.
	The services with problem status values are divided into those with acknowledged problems, those running on hosts that are DOWN, and the rest (unhandled). Click the appropriate link to show details of only those services: • <#> Unhandled Problems • <#> on Problem Hosts (problem services on DOWN hosts) • <#> Acknowledged Each link displays the Service Status Details view for the appropriate services – see *Service Detail*, page 2-26. See *Example: Acknowledging a Problem*, page 2-115, for information on acknowledging a problem.
Monitoring Features	Indication of whether or not Notifications and Active Checks are enabled. (Flap Detection is not used by RISS. Event Handlers and Passive Checks, enabled by default, are also *not used*.)
	Click the Enabled/Disabled indication of a monitoring feature to display the External Command Interface, where you can disable or enable the feature – see *Example: Enabling/Disabling Notifications*, page 2-115.

Related Views

- The charts Hosts and Services in the Tactical Overview view repeat information available in the charts Host Status Totals and Service Status Totals of other views – see *Status Summary*, page 2-11.
- The following views provide more extensive information on monitoring performance:
  - *Nagios Stats*, page 2-42
  - *Hostgroup Information*, page 2-100
- You use the command Acknowledge this host/service problem in the Host/Service Information view to acknowledge a host/service problem. See *Example: Acknowledging a Problem*, page 2-115.

Table 2-19: Links **To** the Tactical Overview View

Origin	Link
left menu	Tactical Overview

Table 2-20: Links **From** the Tactical Overview View

Destination	Link
Nagios Stats, page 2-42	Monitoring Performance
Service Detail, page 2-26, for all hosts or services with the specific status value	host or service status value
External Command Interface, page 2-114	Enabled/Disabled

View Cell Space

The View Cell Space view lets you determine the status of the data-archiving system, by providing information on the hosts involved directly with the active-archive application.

Note: For monitoring purposes, you normally do *not* need to use this view. It is intended for use by system installers and advanced system administrators.

The following table describes the View Cell Space view features.

Table 2-21: View Cell Space View Features

Feature	Description
• SMTP Portals • HTTP Portals • MetaServer • TSC-NAT	Names of the hosts in each of these host groups Click a name to display the Agent view for the host.

Table 2-21: View Cell Space View Features (Continued)

Feature	Description
domains	Smart cells of each domain, organized by smart cell group. Information for each smart cell group: • Unique smart cell group identification number (generated automatically by RISS) • Host names of the smart cells in the smart cell group, prefixed by **P-**, for the primary cell, **S-**, for the secondary cell, and **R**- for a replication cell. • The life cycle state of each smart cell. See *Smart Cell Life Cycle State Definitions*, page 1-4. If the state of a cell cannot be determined, this is indicated by a note that the primary (or secondary) cell is lost. • The background color indicates the current life cycle state of a smart cell in a general way, as follows: – green (normal state): ASSIGNED, CLOSED, FREE – yellow (maintenance state): DISCOVERY, COMPLETE_PROCESSING, BACKING_UP, SYNC_WAIT, RESET, RESTORE – red (failure state): DEAD, SUSPENDED
	Click a smart cell name to display the Agent view for the cell.
Unaffiliated Smart Cells	Smart cells not currently affiliated with any domain (so, not belonging to a smart cell group). These are reserve cells that you can put to use when needed. The cell descriptions are the same as those in the domain lists (see previous). Unaffiliated cells are in either the FREE or the RESET life cycle state.
	Click a smart cell name to display the Agent view for the cell.

Related Views

- Much of the smart cell information in the View Cell Space view is also provided by the Smart Cell Groups for Domain view – see *Smart Cell Groups for Domain*, page 2-112.

Table 2-22: Links **To** the View Cell Space View

Origin	Link
left menu	View Cell Space

Table 2-23: Links **From** the View Cell Space View

Destination	Link
Agent, page 2-111	• host name • Back to Agent View
MBean, page 2-110	Back to MBean View

Service Detail

The Service Status Details view provides detailed service information for a specific host, all hosts in a host group, or all hosts in the system.

Charts Host Status Totals and Service Status Totals of the Service Status Details view are the same as those of the Status Summary view – see *Status Summary*, page 2-11, with the following exception:

Note: Clicking a status value column heading in the Host Status Totals chart displays the Service Status Details view, filtered to show only the services running on hosts with that host status value (it does *not* display the Status Overview view).

The chart Service Status Details provides information on each of the services running on the target host(s). Some of the chart column headings have associated vertical arrows. To sort the chart in ascending order for a given column, click the orange up arrow; to sort it in descending order, click the green down arrow.

The following table describes the Service Status Details chart features.

Table 2-24: Service Status Detail View, Service Status Details Chart Features

Feature	Description
Host	Target hosts. Host health is indicated by color coding – see *Host Status Value Definitions*, page 1-6. Icons indicate the presence of a comment () and/or scheduled downtime ().
	Click a host name, such as sc-sc1-172-1, to display status information for that host. See *Host Information*, page 2-103.
Service	Services running on each target host. Service health is indicated by color coding – see *Service Status Value Definitions*, page 1-7.
	Click a service name, such as PING, to display status information for that service. See *Service Information*, page 2-106.
Status	Current status values of the services. See *Service Status Value Definitions*, page 1-7.
Last Check	Time the service was last checked
Duration	Length of time the service has been running
Attempt	Number of successful attempts, and total number of attempts, to check the service
Status Information	Additional information on the health of the service

Related Views

- The Service Problems view is a subset of the Service Status Details view, providing information about only those services that have problems – see *Service Problems*, page 2-34.

Table 2-25: Links **To** the Service Status Details View

Origin	Link
left menu	Service Detail

Table 2-25: Links **To** the Service Status Details View (Continued)

Origin	Link
Status Summary, page 2-11	• View Service Status Detail . . . • status column heading, Service Status Totals chart (shows services with that status value) • host status value in chart Status Summary For All Host Groups (shows services running on hosts with that status value) • service status value in chart Status Summary For All Host Groups (shows services with that status value)
Host Detail, page 2-30	• View Service Status Detail . . . • status column heading, chart Service Status Totals (filters view to show only services with that status value)
Host Problems, page 2-35	• View Service Status Detail . . . • status column heading, chart Service Status Totals (filters view to show only services with that status value)
Status Overview, page 2-32	• View Service Status Detail . . . • status column heading, chart Service Status Totals (shows services with that status value) • host name, or host status-signal icon (), chart Service Overview . . . • Services entry, chart Service Overview . . .
Status Grid, page 2-108	• View Service Status Detail . . . • status column heading, chart Service Status Totals (shows services with that status value) • host group name, chart Status Grid For . . . • host status-signal icon (), chart Status Grid For . . .
Trends, page 2-51, for *host* trends	View Status Detail For This Host
Availability, page 2-55, for a single host	View Status Detail For This Host
Alert Histogram, page 2-60	View Status Detail For This Host
Alert History, page 2-64	View Status Detail . . .

Table 2-25: Links **To** the Service Status Details View (Continued)

Origin	Link
Notifications, page 2-71, for single host, or when gray-box heading is Notifications	View Status Detail . . .
Service Problems, page 2-34	• View Host Status Detail . . . • status column heading, Host Status Totals chart (filters view to show only services running on hosts with that host status value)
Hostgroup Information, page 2-100	View Status Detail For This Hostgroup
Service Information, page 2-106	View Status Detail For This Host
Host Information, page 2-103	View Status Detail For This Host
Tactical Overview, page 2-21	specific status values for hosts or services
Nagios Stats, page 2-42	Active Service Checks (<#> Total)
Scheduling Queue, page 2-43	specific service name
Service Status Details	status column heading, chart Host Status Totals (filters view to show only services running on hosts with that host status value)
Service Detail	status column heading, chart Service Status Totals (filters view to show only services with that service status value)

Table 2-26: Links **From** the Service Detail View

Destination	Link
Service Information, page 2-106	service name
When main heading is Service Status Details For . . . *<hostgroup(s)>*	
Status Summary, page 2-11	View Host Status Summary . .

Table 2-26: Links **From** the Service Detail View (Continued)

Destination	Link
Host Detail, page 2-30	View Host Status Detail . .
Status Overview, page 2-32	View Status Overview . .
Status Grid, page 2-108	View Host Status Grid . .
When main heading is Service Status Details For All Hosts	
Alert History, page 2-64	View History For All Hosts
Notifications, page 2-71	View Notifications For All Hosts
Host Detail, page 2-30	View Host Status Detail For All Hosts

Host Detail

The charts Host Status Totals and Service Status Totals of the Host Detail view are the same as those of the Status Summary view – see *Status Summary*, page 2-11.

The chart Host Status Details provides status information on a specific host, all hosts in a host group, or all hosts in the system. Some of the chart column headings have associated vertical arrows. To sort the chart in ascending order by a given column, click the orange up arrow; to sort the chart in descending order by a given column, click the green down arrow.

The following table describes the Host Status Details chart features.

Table 2-27: Host Detail View, Host Status Details Chart Features

Feature	Description
Host	Target hosts. Icons indicate the presence of a comment () and/or scheduled downtime ().
	Click a host name, such as sc-sc1-172-1, to display status information for that host. See *Host Information*, page 2-103.
Status	Current status values of the host. See *Host Status Value Definitions*, page 1-6.
Last Check	Time the host was last checked

Table 2-27: Host Detail View, Host Status Details Chart Features (Continued)

Feature	Description
Duration	Length of time the host has been running
Status Information	Additional information on the status of the host

Related Views

- The Host Problems view is a subset of the Host Detail view, providing information about only those hosts that have problems – see *Host Problems*, page 2-35.

Table 2-28: Links **To** the Host Detail View

Origin	Link
left menu	Host Detail
Status Summary, page 2-11	View Host Status Detail . . .
Service Detail, page 2-26, when main heading is Service Status Details For . . . *<hostgroup(s)>*	View Host Status Detail . . .
Status Overview, page 2-32	View Host Status Detail . . .
Status Grid, page 2-108	View Host Status Detail . . .
Scheduling Queue, page 2-43	host name

Table 2-29: Links **From** the Host Detail View

Destination	Link
Service Detail, page 2-26	View Service Status Detail . . .
Status Overview, page 2-32	View Status Overview . . .
Status Summary, page 2-11	View Status Summary . . .
Status Grid, page 2-108	View Status Grid . . .
Hostgroup Information, page 2-100	host group abbreviation, in parentheses – example: (sc)

Status Overview

The Status Overview view lets you see the status of each host in a single host group or all host groups. For each of these hosts, it also shows the number of services that have each service status value.

The charts Host Status Totals and Service Status Totals of this view are the same as those of the Status Summary view – see *Status Summary*, page 2-11.

The chart Service Overview For <*hostgroup(s)*> provides information on the status values of the hosts and services in the host groups displayed. These are described for a single host group in the following table.

Table 2-30: Status Overview View, Host Group Features

Feature	Description
chart title	The host group name (for example SmartCells) and its abbreviation (for example, sc).
Host	Hosts in the host group.
	Click a host name, such as sc-sc1-172-1, to display the Service Detail view filtered for that host. See *Service Detail*, page 2-26.
Status	Current status value of the host. See *Host Status Value Definitions*, page 1-6.
Services	How many services running on the host have each status value (counts of zero are omitted). For example, 6 OK means six services are functioning correctly.
	Click an entry, such as 6 OK, to display the Service Status Details view filtered for that host and service status value. See *Service Detail*, page 2-26.
Actions (two buttons): • View Extended Information For This Host () • View Service Details For This Host ()	• Displays the Host Information view for the host – see *Host Information*, page 2-103. • Same as clicking the host name (see Host, above).

Related Views

- The Status Summary view information is a subset of the Status Overview view information – see *Status Summary*, page 2-11. The Status Summary view provides only the number of hosts having each status value; the Status Overview view provides the status value of each host. Use the Status Overview for information on individual hosts.

Table 2-31: Links **To** the Status Overview View

Origin	Link
left menu	Status Overview
Status Summary, page 2-11	• View Status Overview . . . • host group name (shows overview of that host group) • status column heading, Host Status Totals chart (shows overview of that status value, for all host groups)
Host Detail, page 2-30, and *Host Problems*, page 2-35	• View Status Overview . . . • status column heading, Host Status Totals chart (shows overview of that status value, for all host groups)
Service Detail, page 2-26, when main heading is Service Status Details For . . . *<hostgroup(s)>*	View Status Overview . . .
Status Grid, page 2-108	• View Status Overview . . . • status column heading, Host Status Totals chart (shows overview of that status value, for all host groups)
Hostgroup Information, page 2-100	View Status Overview For This Hostgroup
Status Overview	status column heading, Host Status Totals chart (shows overview of that status value, for all host groups)

Table 2-32: Links **From** the Status Overview View

Destination	Link
Service Detail, page 2-26	View Service Status Detail . . .

Table 2-32: Links **From** the Status Overview View (Continued)

Destination	Link
Host Detail, page 2-30	View Host Status Detail . . .
Status Summary, page 2-11	View Status Summary . . .
Status Grid, page 2-108	View Status Grid . . .

Service Problems

The Service Problems view is a subset of the Service Status Details view, providing information about only those services that have problems – see *Service Detail*, page 2-26.

See Also

- *Detailed Email Reports*, page 2-47, for information on automatically sending email reports containing the same information as the Service Problems view.

Table 2-33: Links **To** the Service Problems View

Origin	Link
left menu	Service Problems
Status Summary, page 2-11	All Problems, in chart Host Status Totals or Service Status Totals
Service Detail, page 2-26	All Problems, in chart Host Status Totals or Service Status Totals
Status Overview, page 2-32	All Problems, in chart Host Status Totals or Service Status Totals
Status Grid, page 2-108	All Problems, in chart Host Status Totals or Service Status Totals
Host Detail, page 2-30	All Problems, in chart Service Status Totals

Table 2-34: Links **From** the Service Problems View

Destination	Link
Alert History, page 2-64	View History For All Hosts
Notifications, page 2-71	View Notifications For All Hosts
Service Detail, page 2-26	View Host Status Detail For All Hosts
Service Information, page 2-106	service name

Host Problems

The Host Problems view is a subset of the Host Status Details view, providing information about only those hosts that have problems – see *Host Detail*, page 2-30.

See Also

- *Detailed Email Reports*, page 2-47, for information on automatically sending email reports containing the same information as the Host Problems view.

Table 2-35: Links **To** the Host Problems View

Origin	Link
left menu	Host Problems

Table 2-36: Links **From** the Host Problems View

Destination	Link
Service Detail, page 2-26	View Service Status Details For All Host Groups
Status Overview, page 2-32	View Status Overview For All Host Groups
Status Summary, page 2-11	View Status Summary For All Host Groups
Status Grid, page 2-108	View Status Grid For All Host Groups

Comments

The Comments view displays all current host and service comments, and lets you add or delete comments. Comments are notes you make to yourself or other system administrators. The gray-box heading for this view is All Host and Service Comments.

Adding Comments

You can add a new host or service comment by clicking the appropriate Add a new host/service comment link. This displays the External Command Interface view, where you enter the new comment – see *Example: Adding a New Comment*, page 2-115.

Note: 1. You must enter host and service names exactly as they appear in PCC views.
2. When adding a comment, the Persistent check box is *not used*. PCC comments are always persistent. They are preserved when the PCC shuts down.

After adding a comment, a cloud-callout icon ( ) appears next to the host or service entry in various views, such as Host Status Details and Service Status Details.

Deleting Comments

You can delete a comment by clicking the wastebasket icon ( ) in its Actions column. This displays the External Command Interface view, where you confirm the deletion.

Related Views

- *Host Information*, page 2-103, also lets you view, add, and delete comments for a given host.
- *Service Information*, page 2-106, also lets you view, add, and delete comments for a given service.

Table 2-37: Links **To** the Comments View

Origin	Link
left menu	Comments

Table 2-38: Links **From** the Comments View

Destination	Link
External Command Interface, page 2-114	Add a new host/service comment

Downtime

The Downtime view lets you view and schedule host and service downtimes, to disable notifications during periods the target hosts and services are down. Scheduled downtimes are generally periods of planned outage, but you can also schedule downtime for a host or service that is already down.

Note: The only effect of a scheduled downtime is to suppress sending notifications; in particular, services are *not* disabled during a downtime.

Since services are not disabled during downtimes, scheduling a downtime for a host also has the effect of scheduling equivalent downtimes for all of its services. When a host is down, checks of its services fail, causing the host itself to be checked. Detected failure of the host then leads to a single notification about the host being down; no service notifications are produced. If the host is scheduled for a downtime, this host notification is suppressed; no notifications are sent at all.

Scheduled downtimes are preserved across PCC shutdowns and restarts.

Disabling Notifications by Scheduling Downtimes

To disable notifications during periods that you expect a host or service to be down, you schedule a downtime for the host or service by clicking the Schedule host downtime or Schedule service downtime link. This displays the External

Command Interface view, where you provide the start and end times for the downtime, and some identifying information (host, service, you, comment) – see *External Command Interface*, page 2-114.

Note: All fields in red, including Comment, are required. If you do not enter a comment, you are informed simply that "an error occurred while processing your command".

To ensure that the start and end times you specify are respected exactly, turn *on* the Fixed check box. When this is turned *off*, the scheduled downtime is flexible: it starts between the start and end times as soon as a problem is detected (UNREACHABLE or DOWN status value for a host, non-OK for a service); the downtime then lasts for the Duration you specify. (Duration is ignored for Fixed downtime.)

After scheduling a downtime, a snore icon () appears next to the host or service entry in various views, such as Host Status Details and Service Status Details.

Reenabling Notifications by Deleting Scheduled Downtimes

You can reenable suppressed notifications by by deleting a scheduled downtime. You do this by clicking the wastebasket icon () in the Actions column. This displays the External Command Interface view, where you confirm the deletion.

Related Views

- *Host Information*, page 2-103, also lets you schedule and delete scheduled host downtime.
- *Service Information*, page 2-106, also lets you schedule and delete scheduled service downtime.
- *Scheduling Queue*, page 2-43, displays scheduled host and service checks, and lets you schedule checks.
- *Nagios Info*, page 2-39, lets you inhibit notifications for all hosts and services. This is *not* for a limited period, however. Notification remains globally disabled until you enable it again.

Table 2-39: Links **To** the Downtime View

Origin	Link
left menu	Downtime

Table 2-40: Links **From** the Downtime View

Destination	Link
External Command Interface, page 2-114	Schedule host/service downtime

Nagios Info

The Nagios Info view provides information about Nagios, the PCC process that monitors hosts and services. The gray-box heading for this view is Nagios Process Information.

The following tables describe the Nagios Info view features. Several features of this view are *not used* by PCC. Only features that are used are described.

Program Information Chart

Table 2-41: Program Information Chart, Nagios Info View

Variable	Description
Program Start Time	Time when PCC was started
Total Running Time	Length of time PCC monitoring has been running since the Program Start Time
Nagios PID	Identifier (PID) of the Nagios Linux process
Notifications Enabled?	Whether or not notifications are currently enabled, in general. Even if this is Yes, notifications can be disabled for individual hosts or services. If this is No, however, notifications are disabled for all hosts and services.
Service Checks Being Executed?	Whether or not PCC is currently monitoring services, in general. Even if this is Yes, checks of individual services can be disabled. If this is No, however, *no* services are checked.

Table 2-41: Program Information Chart, Nagios Info View (Continued)

Variable	Description
Running As A Daemon?	Whether or not the monitoring process (Nagios) is running as a daemon. This is always Yes.
Last External Command Check	Time of the latest execution of an external command – see *External Command Interface*, page 2-114. (When you submit a command, a short delay can elapse before the Control Center executes it.)
Last Log File Rotation	Time and date of the latest event log file rotation. During daily rotation the file is copied from the log directory, `/var/log/nagios`, to the log archive directory, `/var/log/nagios/archives`. The log file is of limited size; when full, the oldest log entries are discarded to make room for new entries. The file is rotated daily to provide a record of past entries.

Some of the Program Information chart variables appear in the Process Commands box as commands to change the current values.

Process State Information Chart

Table 2-42: Process State Information Chart, Nagios Info View

Variable	Description
Process Status	Status of the monitoring process (Nagios). Should be OK; if not, use the command Restart the Nagios process – see *Process Commands Box*, page 2-40. Process status values are the same as service status values – see *Service Status Value Definitions*, page 1-7.

Process Commands Box

The Process Commands box lets you run commands to perform actions. These actions are global, affecting all hosts and all services. For example, if you disable notifications here, no notifications will be sent for any hosts or services.

Commands with an adjacent X icon ( ) or check-mark icon ( ) are toggles. The new toggle state (after command execution) is indicated by the icon: a check mark means enable or start; an X means disable or stop. For example, after you use the command Enable notifications, notifications are enabled and the command Disable Notifications replaces Enable notifications in the Process Commands box.

Click a command link to display the External Command Interface view for the command – see *External Command Interface*, page 2-114.

Commands that disable (notifications, status checks, and so on) override commands that enable. For example, suppose you disable checks for a particular service such as PING using the Service Information view (command Disable checks of this service), but you enable checks for all services using the Nagios Info view (command Start executing service checks). The particular service (PING) is *not* checked, because disabling overrides enabling.

Related Views

- For information on commands that affect only specific host groups, hosts, and services, see Hostgroup Commands, *Hostgroup Information*, page 2-100; Host Commands, *Host Information*, page 2-103; and Service Commands, *Service Information*, page 2-106, respectively.
- You can disable notifications for a single host or service over a defined period by scheduling downtime for it – see *Downtime*, page 2-37.

Table 2-43: Links **To** the Nagios Info View

Origin	Link
left menu	Nagios Info

Table 2-44: Links **From** the Nagios Info View

Destination	Link
External Command Interface, page 2-114	command (See Process Commands Box.)

Nagios Stats

The Nagios Stats view provides information on the performance of service monitoring. The gray-box heading for this view is Performance Information.

The following table describes the Nagios Stats view features.

Table 2-45: Nagios Stats View Features

Feature	Description
Time Frame/ Checks Completed	The number and percentage of PCC services checked in each of the indicated time frames (since PCC startup or in the last 1, 5, 15, or 60 minutes).
Metric/Min/Max/Average • Check Execution Time • Check Latency	The minimum, maximum and average times • it took to check a service • between the time a service check was scheduled and the time it was executed (Percent State Change is *not used*.)

The Passive Service Checks charts are *not used*; all PCC service checks are active.

Related Views

- *Hostgroup Information*, page 2-100, presents the same monitoring performance information, but for only a single host group (and it lets you execute host group commands).
- *Tactical Overview*, page 2-21, also provides (limited) information on monitoring performance.

Table 2-46: Links **To** the Nagios Stats View

Origin	Link
left menu	Nagios Stats
Tactical Overview, page 2-21	Monitoring Performance

Table 2-47: Links **From** the Nagios Stats View

Destination	Link
Service Detail, page 2-26	Active Service Checks (<#> Total)

Scheduling Queue

The Scheduling Queue view lets you view and schedule service checks. It provides information on when each service on each host is scheduled to be checked. The gray-box heading for this view is Service Check Scheduling Queue.

The current sort order is indicated by the heading above the chart – for example, Entries sorted by next check time (ascending). Some of the chart column headings have associated vertical arrows. To sort the chart in ascending order by a given column, click the orange up arrow. To sort the chart in descending order by a given column, click the green down arrow. By default, the chart is sorted by Next Check time in ascending order.

The following table describes the Scheduling Queue view features.

Table 2-48: Scheduling Queue View Features

Feature	Description
Host	Hosts in the system that are scheduled to be checked
	Click a host name, such as sc-sc1-172-1, to display status information for that host. See *Host Information*, page 2-103.
Service	Services scheduled to be checked
	Click a service name, such as PING, to display status information for that service. See *Service Information*, page 2-106.
Last Check	Time the service was last checked
Next Check	Time the service is scheduled to be checked next
Active Checks	Whether the service is being monitored (ENABLED) or not (DISABLED). (All PCC checks are active, not passive, checks.)

Table 2-48: Scheduling Queue View Features (Continued)

Feature	Description
Actions	Click the X icon () or check-mark icon () to, respectively, disable or enable service checks. This displays the External Command Interface view, where you confirm enabling or disabling – see *External Command Interface*, page 2-114.
	Click the wristwatch icon () to reschedule the service. This displays the External Command Interface view, where you reschedule the service. If you turn *on* the check box Force Check in the External Command Interface view, the service will be checked at the newly scheduled time even if the service is disabled at that time.

Table 2-49: Links **To** the Scheduling Queue View

Origin	Link
left menu	Scheduling Queue

Table 2-50: Links **From** the Scheduling Queue View

Destination	Link
Host Information, page 2-103	host name
Service Information, page 2-106	service name
External Command Interface, page 2-114	Actions icon – see above

EmailReporter

The EmailReporter view lets you configure summary monitoring reports to be sent periodically to email recipients you choose. You choose the types of report to send and how often to send them. The main heading for the EmailReporter view is EmailReporter Configuration.

For each type of report (ReportTypes), Detailed and TextSummary, you can choose a reporting period (NotificationGroups) and any number of email recipients (Members). For example, you might decide to make all of the following configuration choices:

- Send a Detailed report Once_A_Day to `ddiderot@ncyclo.com` and `ghegel@yinyangquanta.org`.
- Send a TextSummary report Every_Two_Hours to `myself@myisp.com`.
- Send a TextSummary report Every_Eight_Hours to `mycolleague@isp.com`.

The following table describes the features of the EmailReporter view to create or edit email report configurations.

Table 2-51: EmailReporter View Features

Feature	Description
ReportTypes	The currently configured email report types Select a report type: • Detailed: an HTML report of host and service problems, smart cell information, performance graphs, and exceptions – see *Detailed Email Reports*, page 2-47. • TextSummary: a plain-text ASCII report of domain-specific information such as storage size; host and service problems; and locations of exceptions – see *Text Summary Email Reports*, page 2-50. Suitable for mobile email devices. If the type of report you want to configure is not yet listed, select it in the pulldown list and click Add. To cancel all Detailed or all TextSummary email reports, select the type to cancel and click Delete.

Table 2-51: EmailReporter View Features (Continued)

Feature	Description
NotificationGroups	The currently configured email report periods Choose how often to send the email report: • Every_Two_Hours • Every_Four_Hours • Every_Six_Hours • Every_Eight_Hours • Every_Ten_Hours • Twice_A_Day • Once_A_Day If the period you want is not listed as one of the NotificationGroups, select it in the pulldown list and click Add. To cancel all email reports scheduled for a given period, select the period to cancel (such as Once_A_Day) and click Delete.
Members	The recipient email addresses for the report corresponding to the selected ReportTypes and NotificationGroups fields. To add a recipient, enter the email address and click Add. To remove a recipient, select the email address and click Delete.

To create or edit email report configurations:

1. Check a given report configuration, select its entries in the ReportTypes and NotificationGroups fields. The report recipients are then listed in the Members field.
2. Select different NotificationGroups or Members as needed.
3. Click Submit Configuration to save your configuration changes.

See Also

- *Detailed Email Reports*, page 2-47, and *Text Summary Email Reports*, page 2-50, for information on interpreting the report emails.

Related Views

- *System Status*, page 2-14, provides similar information to that in email reports.

Table 2-52: Links **To** the EmailReporter View

Origin	Link
left menu	EmailReporter

Links *from* the EmailReporter view: none.

Detailed Email Reports

A detailed email report provides system status and performance information in the form of an HTML document. The advantages of the detailed HTML format over the text summary report are that more content is provided and the format is more sophisticated, providing tables and graphics.

The following information is provided in the detailed report:

- Appliance Performance – Information available through the System Status view (see *System Status*, page 2-14).
  - For each domain: the number of messages stored, rate of messages stored, rate of messages replicated, and number of signatures stored (if backup is enabled).
  - For the system (all domains): the total number of messages stored, average rate of messages stores, average rate of messages replicated, and number of signatures stored (if backup is enabled).
  - Number of messages in the system **catch-all repository**. This includes messages too large to be indexed, messages that cannot be parsed, and messages that cannot be routed to a registered RISS user.

    Messages that cannot be parsed include those that have malformed message structure (MIME) and those that use unsupported character sets.

    Messages that cannot be routed are those that do not correspond to any system routing rule. They are not recognized as destined for a registered RISS user. Mailing-list messages cannot be routed if the recipient name is not included in the message as a destination.
  - Store Rate graph – Number of store operations per second, measured hourly over the current day, starting at midnight. This graph is one of the Application Performance Info graphs that are available from the System

Status view, Other Graphs link, with Display Type: Min/Max/Avg and Time Frame: Hours in a day.

- Host Problems – A subset of information in the Host Detail view, providing information only on hosts that have problems (see *Host Detail*, page 2-30).
- Service Problems – A subset of information in the Service Detail view, providing information only on services that have problems (see *Service Detail*, page 2-26).
- Smart Cell Metrics – A subset of the Smart Cell Groups for Domain view (see *Smart Cell Groups for Domain*, page 2-112). This includes for each domain, the following metrics for each smart cell in each smart cell group:
  - Role – Whether the smart cell is the primary, secondary, or first or second replica of the smart cell group.
  - HostName – IP address of the smart cell.
  - State – Current life cycle state of the smart cell – see *Smart Cell Life Cycle State Definitions*, page 1-4.
  - NumArchived – Number of messages archived by the smart cell since it was assigned.
  - NumIndexed – Number of messages indexed by the smart cell since it was assigned.
  - NumFailedDocs – Number of messages that did not get indexed by the smart cell since system startup.
  - NumBackedUpDocs – Number of messages that were backed up by the smart cell since system startup (if the backup option is installed).
  - Store Rate – Rate (per second) of storage operations on the smart cell at the time of the report.
- Free Smart Cells – List of smart cells in the free state at the time of the report.
- Domain Configuration – For each domain: the set size (number of groups that can be created), the disabled/enabled state of compliance, backup, and replication, and the replica count (number of replicas that will be created for each group).

- Software Versions – Versions of RISS software currently installed, including:
  - Application – third-party software package, also called L3.
  - Installer – the RISS installation program.
  - Linux and Windows Cores – RISS and operating system software on Linux and Windows servers, also called L2 and W2, respectively,
  - Windows System – Windows software, also called W3.
- Installed Patches – RISS software patches that have been installed.

In addition to the information in the report itself, plain-text attachments provide the exception logs for the following host groups:

- `SmartCell_Exceptions.txt` – Smart cells host group
- `MetaServer_Exceptions.txt` – Metaserver host group
- `HTTP_Exceptions.txt` – HTTP portals host group
- `SMTP_Exceptions.txt` – SMTP portals host group
- `LogServer_Exceptions.txt` – TSC-NAT host group

This is the same information available through the Exceptions field links of the System Status view. If no exceptions have occurred since startup of the respective servers, there is no link and accordingly no log attached to the detail report. Any exceptions older than those in the attachments were pruned from the event log when it filled up.

See Also

- *Text Summary Email Reports*, page 2-50, for information on text summary email reports
- *Host Problems*, page 2-35
- *Service Problems*, page 2-34
- *Smart Cell Groups for Domain*, page 2-112
- *System Status*, page 2-14

Text Summary Email Reports

A text summary email report provides a short, plain-text summary of system status and performance information. The advantage of the plain-text format and small message size over the detailed HTML report is that you can access the text summary from wireless handheld email devices.

The following information is provided in the plain-text summary report:

- Report identification: date and time; site name.
- The versions of RISS software currently used: Spine (also called L2: foundation software, including operating systems), Application (also called L3), and Installer.
- For each domain (DOMAIN SPECIFIC INFORMATION):
  - Domain name
  - Number of smart cell groups (SetSize)
  - Whether or not the system is ready for storage operations (SMTP portals are ready and smart cells are allocated for this domain)
  - Whether or not the system is currently storing
  - Whether or not the system is currently backing up data
  - Whether or not the system is currently backing up message signatures
  - Size in gigabytes of the raw data (documents) to be stored, before compression
  - Percentage disk utilization

- Number of FREE smart cells, total number of smart cells, FREE/total ratio as a percentage
- Hosts that currently have problems
- Services that currently have CRITICAL problems (and their hosts)
- Host groups where exceptions are currently logged (same as Exceptions field link names of System Status view – see *System Status*, page 2-14)

See Also

- *Detailed Email Reports*, page 2-47, for information on detailed HTML email reports
- *System Status*, page 2-14

Trends

The Trends view lets you create reports on the status of individual hosts or services over given time periods.

How To Create a Trends Report

1. Choose the report type: Host or Service.
2. Choose a host or service.
3. Choose the report options. You typically choose the Report Period (first option) and use the default values for the other options.
   - Report Period – Choose a predefined period (Last 24 Hours, Today, Yesterday, This Week, Last 7 Days, Last Week, This Month, Last Month, This Year, Last Year); or choose * CUSTOM REPORT PERIOD * and specify the custom report start and end dates.
   - Assume Initial States – Choose Yes to assume that any undetermined status value is really the First Assumed State. Choosing No is equivalent to choosing Yes and choosing Unspecified as the First Assumed State.
   - Assume State Retention – Choose Yes to use the last recorded status value before PCC startup as the status value to assume for periods when monitoring was down.

- First Assumed State – Choose the status value to assume for periods when monitoring was down. Has no effect if Assume Initial States is No or Assume State Retention is Yes.
- Backtracked Archives – *Not used*
- Suppress image map – Turn this on to inhibit zooming into the State History chart by clicking a status color.
- Suppress popups – Turn this on to inhibit display of tooltips in State History chart status bars.

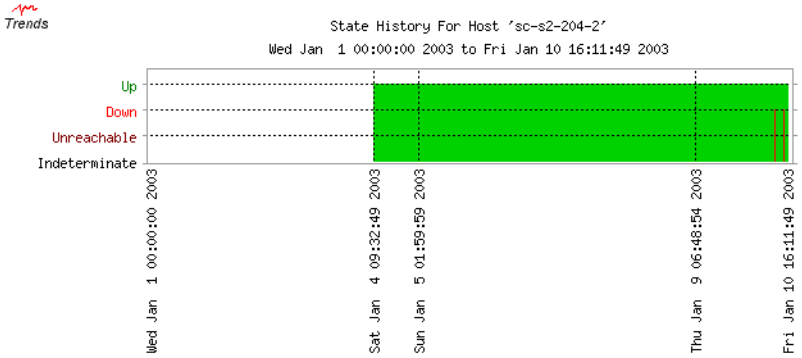
4. Click Create Report to create the report.

The following table describes the Trends report features.

Table 2-53: Trends Report Features

Feature	Description
heading	• Name of the host or service reported on • The covered report period

Table 2-53: Trends Report Features (Continued)

Feature	Description
State History	A color-coded chart indicating the host/service status value trends over the reported time period  Pause the mouse pointer over a status bar to display a tooltip of additional information. (Pausing has no effect if Suppress popups is turned *on* – see *How To Create a Trends Report*, page 2-51.) Example tooltip: **DOWN** **Time Range**: *Fri Dec 6 09:10:49 2002 to Fri Dec 6 09:14:21 2002* **Duration**: *0d 0h 3m 32s* **State Info**: *CRITICAL - Plugin timed out after 10 seconds* Click a status color in the Status History chart to zoom in by the Zoom factor (see below). (Clicking has no effect if Suppress image map is turned *on* – see *How To Create a Trends Report*, page 2-51.)
State Breakdowns	Summary chart showing the total elapsed time for each host or service status value since startup of PCC monitoring (in parentheses, this is expressed as a percentage of total time).

The same color coding is used in both charts: State History and State Breakdowns. For descriptions of the possible status values, see *Host and Service Status Value Definitions*, page 1-6. The additional value Indeterminate used in these charts generally indicates time that the entire system (site) was not operational.

In addition to the report features described above, the report view has an input form at the upper right that you can use to update the report. After changing report options, click the Update button to regenerate the report with the new options.

The input form options you can set are the same as those you used to create the displayed report: Assume initial states, Report period, and so on, with the addition of the Zoom factor. The Zoom factor affects how much each mouse click zooms into the Status History chart (see State History feature, above). A larger factor zooms more.

Related Views

- *Availability*, page 2-55, lets you create a report on the availability of individual hosts, services, or host groups over given time periods.
- *Alert History*, page 2-64, shows logged alerts.
- *Alert Histogram*, page 2-60, shows the number of alerts of different types for hosts and/or services.

Table 2-54: Links **To** the Trends View

Origin	Link
left menu	Trends
Availability, page 2-55, for a single host or service	• View Trends For This Host/Service • status bar chart
Alert Histogram, page 2-60	View Trends For This Host/Service
Alert History, page 2-64, for a single host or service	View Trends For This Host/Service
Notifications, page 2-71, for a single host or service	View Trends For This Host/Service
Host Information, page 2-103	View Trends For This Host
Service Information, page 2-106	View Trends For This Service
Trends view of a service	View Trends For This Host

Table 2-55: Links **From** the Trends View

Destination	Link
Trends view for the host this service is running on – when view shows *service* trends	View Trends For This Host
Availability, page 2-55, for this host or service	View Availability Report For This Host/ Service
Alert Histogram, page 2-60, for this host or service	View Alert Histogram For This Host/ Service
Service Detail, page 2-26, for this host – when view shows *host* trends	View Status Detail For This Host
Alert History, page 2-64, for this host or service	View Alert History For This Host/Service
Notifications, page 2-71, for this host or service	View Notifications For This Host/Service

Availability

The Availability view lets you create reports on the availability of individual hosts, services, or host groups, over given time periods.

How To Create an Availability Report

1. Choose the report type: Hostgroup(s), Host(s), or Service(s).
2. Depending on the report type, choose a host group, host, or service; or choose all host groups, hosts, or services.
3. Choose the report options. You will typically choose the Report Period (first option) and use the default values for the other options.
   - Report Period – Choose a predefined period (Last 24 Hours, Today, Yesterday, This Week, Last 7 Days, Last Week, This Month, Last Month, This Year, Last Year); *or* choose * CUSTOM REPORT PERIOD * and specify the custom report start and end dates.
   - Assume Initial States – Choose Yes to assume that any undetermined status value is really the First Assumed State. Choosing No is equivalent to choosing Yes and choosing Unspecified as the First Assumed State.

- Assume State Retention – Choose Yes to use the last recorded status value before PCC startup as the status value to assume for periods when monitoring was down.
- First Assumed State – Choose the status value to assume for periods when monitoring was down. Has no effect if Assume Initial States is No or Assume State Retention is Yes.
- Backtracked Archives – *Not used*
- Turn *on* the check box Output in CSV Format if you want the report in comma-separated value format, instead of HTML. Available only for reports on all hosts or all services. This can be useful if you need to insert the generated report into a spreadsheet.

4. Click Create Availability Report to create the report.

The following tables describe the various availability reports.

Table 2-56: Availability Report Features, Single Host or Service

Feature	Description
heading	• Name of the host or service name reported on. • The covered report period.
Host/Service State Breakdowns	A color-coded history chart indicating the host/service status value trends over the reported time period. This is a reduced version of the corresponding Trends view.  Click the bar chart to display the full Trends view – see *Trends*, page 2-51.
	A chart indicating, for each host or service status value, and for each Type/Reason: • Time – Duration of the status value. • % Total Time – Duration of the status value, as a percentage of the total time since startup of PCC monitoring. • % Known Time – Duration of the status value, as a percentage of the total time since startup of PCC monitoring minus the time with Undetermined status. Each determined status value is divided into Scheduled and Unscheduled periods, depending on whether downtime was scheduled or not. Status can be Undetermined because monitoring was not running at the time, or because there was not enough data available to determine the status value.
State Breakdowns For Host Services (host report only)	For each service running on the host, the percent of total elapsed time for each service status value. Values in parentheses represent percentages of the total time minus the time with Undetermined status.
	Click a service name to view the service Availability report.
Host/Service Log Entries	For each host/service event, event start and end time, duration, type, and descriptive information
	Click the link to toggle between viewing only problem events (condensed log entries) and all logged events (full log entries).

Table 2-57: Availability Report Features, Single Host Group, or All Host Groups, Hosts, or Services

Feature	Description
heading	• Name of the report: the individual host group, or All Hostgroups, Hosts, or Services • The covered report period
Host/Service State Breakdowns For host group reports, Host State Breakdowns are organized by host group.	For each host or service, and each of its status values: % Time <status value> – Duration of the status value, as a percentage of the total time and, in parentheses, as a percentage of the total time minus the time with Undetermined status.

In addition to the report features described above, each report view has an input form at the upper right that you can use to update the report using different options. The options you can set are the same as those you used to create the displayed report: Assume initial states, Report period, and so on. After changing report options, click the Update button to regenerate the report with the new options.

Table 2-58: Links **To** the Availability View

Origin	Link
left menu	Availability
Trends, page 2-51	View Availability Report For This Host/Service
Alert Histogram, page 2-60	View Availability Report For This Host/Service
Hostgroup Information, page 2-100	View Availability Report For This Hostgroup
Host Information, page 2-103	View Availability Report For This Host
Service Information, page 2-106	View Availability Report For This Service
Availability report for single host or service	View Availability Report For All Hosts/Services
Availability report for single service	View Availability Report For This Host
Availability report for single host	service name

All links from the Availability view use the same report options for the destination view as were used for the current availability report.

Table 2-59: Links **From** the Availability View

Destination	Link
From *single* host report	
Availability report for single service	service name
From *single* host or service report	
Availability report for *all* hosts/services	View Availability Report For All Hosts/Services
Trends, page 2-51, for this host or service	View Trends For This Host/Service
Alert Histogram, page 2-60, for this host or service	View Alert Histogram For This Host/Service
Alert History, page 2-64, for this host or service	View Alert History For This Host/Service
Notifications, page 2-71, for this host or service	View Notifications For This Host/Service
From *single host* report	
Service Detail, page 2-26, for this host	View Status Detail For This Host
From *single service* report	
Availability report for the host this service is running on	View Availability Report For This Host

Alert Histogram

The Alert Histogram view lets you create reports with simple graphs showing, for individual hosts or services, the number of events of different types over different time periods.

The following histogram shows all service events over a one-day period. It shows, for example, that two CRITICAL events and three WARNING events occurred around 6:45, and two recovery (OK) events occurred around 7:00.

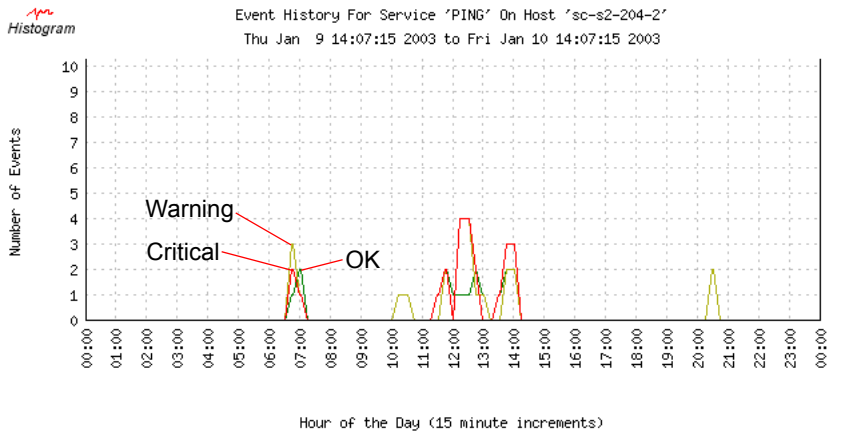


Figure 2-2: Alert histogram of all service events over one-day period

Whenever graph lines for events of different status values overlap exactly, only the most severe status value is indicated. To see an event line that is hidden by overlapping, create a separate histogram for just the hidden status

value. For example, the histogram below shows only the recovery (OK) events for the same time period. The OK event line from 11:15 to 13:15 was hidden by CRITICAL and WARNING event lines in the above histogram.

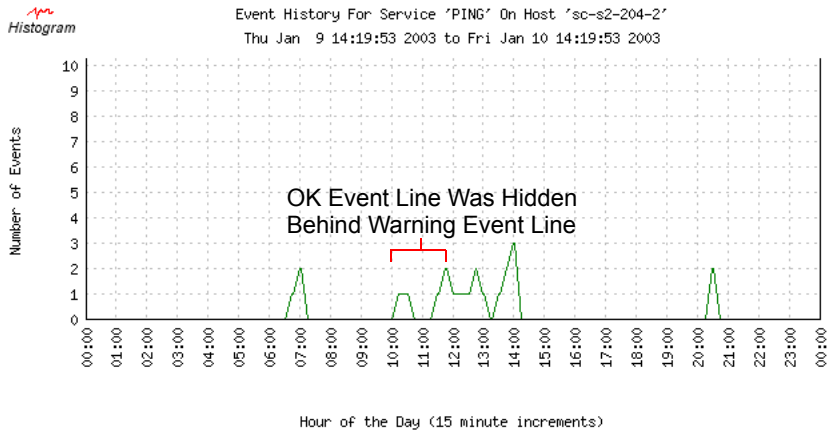


Figure 2-3: Alert histogram of recovery service events over one-day period

How To Create an Alert Histogram Report

1. Choose the report type: Host or Service.
2. Choose the host or service to report on.
3. Choose the report options:
   - Report Period – Choose a predefined period (Last 24 Hours, Today, Yesterday, This Week, Last 7 Days, Last Week, This Month, Last Month, This Year, Last Year); or choose * CUSTOM REPORT PERIOD * and specify the custom report start and end dates.
   - Statistics Breakdown – Choose the time scale to use for the Report Period: Month, Day of the Month, Day of the Week, or Hour of the Day.
   - Events To Graph – Choose the type of host or service events to report on: events indicating change to a specific status value, all problem status values, or all events.
   - State Types To Graph – Choose which status conditions to graph: HARD, SOFT, or both. See *Hard and Soft Status Condition Definitions*, page 1-7.

- Assume State Retention – (Typically, you will use the default value, Yes.) Choose Yes to use the last recorded status value before PCC startup as the status value to assume for periods when monitoring was down.
- Initial States Logged – *Not used*
- Ignore Repeated States – *Not used*

4. Click Create Report to create the report.

The following table describes the Alert Histogram report features.

Table 2-60: Alert Histogram Report Features

Feature	Description
heading	• Name of the host or service reported on • The covered report period
Event History	A color-coded graph indicating the host/service event history over the reported time period. See *Host and Service Status Value Definitions*, page 1-6, for information on color coding of status values.
event breakdowns	Summary chart showing the number of events associated with each host/service status value over the covered time period. Minimum, maximum, total, and average number of events are reported. The same status value colors are used as in the Event History graph.

The same status colors are used in both charts: the graph and the event breakdowns. For descriptions of the possible status values, see *Host and Service Status Value Definitions*, page 1-6.

In addition to the report features described above, the report view has an input form at the upper right that you can use to update the report. After changing report options, click the Update button to regenerate the report with the new options. The input form options you can set are the same as those you used to create the displayed report: Report period, Assume state retention, and so on.

Related Views

- *Trends*, page 2-51, shows status value trends for hosts and/or services.
- *Alert History*, page 2-64, shows a detailed chronology of events for hosts and/or services.

Table 2-61: Links **To** the Alert Histogram View

Origin	Link
left menu	Alert Histogram
Trends, page 2-51, for a specific host or service	View Alert Histogram For This Host/Service
Availability, on page 2-55, for a specific host or service	View Alert Histogram For This Host/Service
Host Information, page 2-103, for a specific host	View Alert Histogram For This Host
Service Information, page 2-106, for a specific service	View Alert Histogram For This Service

Table 2-62: Links **From** the Alert Histogram View

Destination	Link
Trends, page 2-51, for this host or service	View Trends For This Host/Service
Availability, page 2-55, for this host or service	View Availability Report For This Host/ Service
Alert History, page 2-64, for this host or service	View History For This Host/Service
Notifications, page 2-71, for this host or service	View Notifications For This Host/Service
Service Detail, page 2-26, for this host	View Status Detail For This Host

Alert History

The Alert History view provides a chronology of logged PCC alerts. Alerts are a subset of the events listed in the Event Log view. You can filter this view to display only alerts of a specific type, and you can display the alerts for any given day.

The following table describes the Alert History view features.

Table 2-63: Alert History View Features

Feature	Description
Log File Navigation	Day covered by the current view
	Click the left (right) arrow to view alerts from the previous (next) day.
alerts	The information for each alert includes the following: • Color-coded status icon (green: normal, yellow: warning, red: failure, orange: unknown) • Time stamp • Alert type: HOST or SERVICE • Host identifier • Service identifier (service alerts only) • Host or service status value – see *Host and Service Status Value Definitions*, page 1-6 • Status condition (HARD or SOFT) – see *Hard and Soft Status Condition Definitions*, page 1-7 • Sequential identifier for this alert message – indicates how many times it has been sent • Alert message (additional information describing the alert)

Table 2-63: Alert History View Features (Continued)

Feature	Description
update form (upper right)	To update the Alert History view – 1.Choose the following update options: – To show only alerts regarding certain status conditions, choose a condition (SOFT, HARD, All) in the pulldown list State type options. See *Hard and Soft Status Condition Definitions*, page 1-7. – To show only certain types of alerts, choose an alert type in the pulldown list History detail level. For example, choose Service critical to show only alerts for services with status value CRITICAL. – To hide certain types of alerts, turn on the appropriate Hide check box. – To change the alert list order, click the check box Older Entries First. 2.Click Update.

Related Views

- The information in the Alert History view is a subset of that in Event Log view – see *Event Log*, page 2-74.
- *Alert Histogram*, page 2-60, shows the number of alerts of different types for hosts and/or services.
- *Trends*, page 2-51, shows status value trends for hosts and/or services.

Table 2-64: Links **To** the Alert History View

Origin	Link
left menu	Alert History
Service Detail, page 2-26, when main heading is Service Status Details For All Hosts	View History For All Hosts
Service Problems, page 2-34	View History For All Hosts
Notifications, page 2-71 • when gray-box heading is Notifications • single host • single service	View History For: • All Hosts • This Host • This Service
Host Information, page 2-103	View Alert History For This Host

Table 2-64: Links **To** the Alert History View (Continued)

Origin	Link
Service Information, page 2-106	View Alert History For This Service
Trends, page 2-51	View History For This Host/Service
Availability, page 2-55, for single host or service	View History For This Host/Service
Alert Histogram, page 2-60	View History For This Host/Service
Alert History, for single service	View History For This Host

Table 2-65: Links **From** the Alert History View

Destination	Link
When view shows alerts for all hosts and services	
Service Detail, page 2-26	View Status Detail For All Hosts
Notifications, page 2-71	View Notifications For All Hosts
When view shows alerts for a single host or service	
Notifications, page 2-71, filtered for this host/service	View Notifications For This Host/Service
Trends, page 2-51, filtered for this host/service	View Trends For This Host/Service
When view shows alerts for a single host	
Service Detail, page 2-26, filtered for this host	View Status Detail For This Host
When view shows alerts for a single service	
Alert History view, filtered for the host where this service is running	View History For This Host

Alert Summary

The Alert Summary view lets you create reports summarizing different types of alerts over different time periods. You can create any of several standard alert summary reports, or create a custom alert summary report.

How To Create a Standard Alert Summary Report

1. Choose a standard Report Type under Standard Reports. Only alerts with HARD status conditions are reported – see *Hard and Soft Status Condition Definitions*, page 1-7.

   Table 2-66: Standard Alert Summary Report Types

Standard Report Type	Reports on . . .
25 Most Recent Hard Alerts	The 25 most recent HARD host and service alerts. Same as a custom report of type Most Recent Alert (see *Alert Summary Report Features, Most Recent Alerts*, page 2-69), except only HARD alerts are reported.
25 Most Recent Hard Host Alerts	Same as previous, but only HARD *host* alerts are reported.
25 Most Recent Hard Service Alerts	Same as previous, but only HARD *service* alerts are reported.
Top 25 Hard Host Alert Producers	List of the 25 hosts that produced the most HARD alerts, ranked in order of number of alerts produced. Similar to a custom report of type Top Alert Producers see *Alert Summary Report Features, Top Alert Producers*, page 2-70.
Top 25 Hard Service Alert Producers	Same as previous, but reports on services that produced HARD alerts.

2. Click Create Summary Report (under Standard Reports).

How To Create a Custom Alert Summary Report

1. Choose a custom Report Type under Custom Report Options.

Table 2-67: Custom Alert Summary Report Types

Custom Report Type	Reports on . . .
Most Recent Alerts	The 25 most recent alerts, with such details as the alert time and alert message
Alert Totals	Summary information on the number of alerts for each host and service status value
Alert Totals By Hostgroup	Same as Alert Totals, but totals for each host group
Alert Totals By Host	Same as Alert Totals, but totals for each host
Alert Totals By Service	Same as Alert Totals, but totals for each service
Top Alert Producers	The 25 hosts and/or services that produced the most alerts, ranked by number of alerts produced

2. Choose the report options:
   - Report Period – Choose a predefined period (Last 24 Hours, Today, Yesterday, This Week, Last 7 Days, Last Week, This Month, Last Month, This Year, Last Year); or choose * CUSTOM REPORT PERIOD * and specify the custom report start and end dates.
   - Limit To Hostgroup – Choose a host group to report on, or ** ALL HOSTGROUPS **.
   - Limit To Host – Choose a host to report on, or ** ALL HOSTS **.
   - Alert Types – Choose to report on host alerts, service alerts, or both.
   - State Types – Choose to report on alerts concerning HARD, SOFT, or both status conditions – see *Hard and Soft Status Condition Definitions*, page 1-7.
   - Host States – Choose which host status values to report on: UP, DOWN, UNREACHABLE, problem status values (DOWN, UNREACHABLE), or all host status values.
   - Service States – Choose which service status values to report on: OK, WARNING, UNKNOWN, CRITICAL, problem status values (WARNING, CRITICAL), or all service status values.
   - Max List Items – Enter the maximum number of alerts to report.

3. Click Create Summary Report to create the report.

The following table describes the features common to all Alert Summary reports. Subsequent tables describe the features specific to each report type.

Table 2-68: Alert Summary Report Features, General

Feature	Description
heading	Indicates the choice you made for Report Type, together with the time period covered
Report Options Summary	Indicates the other report creation options you chose
	Click Generate New Report to change report options and create a new Alert Summary report.
main chart heading	Brief description of the report contents. Examples: • Displaying most recent 25 of 742 total matching alerts • Totals By Hostgroup
(Remaining fields depend on the type of report. See the appropriate following table.)	

The following table describes the features specific to Alert Summary reports of type Most Recent Alerts. For a description of the fields common to all Alert Summary reports, see *Alert Summary Report Features, General*, page 2-69.

Table 2-69: Alert Summary Report Features, Most Recent Alerts

Feature	Description
Time	Time of the alert
Alert Type	Whether a host or service alert
Host	Name of the host
	Click the host name to display the Host Information view – see *Host Information*, page 2-103.
Service	Name of the service
	Click the service name to display the Service Information view – see *Service Information*, page 2-106.
State	Host/service status value

Table 2-69: Alert Summary Report Features, Most Recent Alerts (Continued)

Feature	Description
State Type	Whether the status condition is HARD or SOFT – see *Hard and Soft Status Condition Definitions*, page 1-7
Information	The alert message

The following table describes the features specific to Alert Summary reports of type Alert Totals (including those organized by host group, host, and service). Totals are given for each possible host or service status value. For a description of the fields common to all Alert Summary reports, see *Alert Summary Report Features, General*, page 2-69.

Table 2-70: Alert Summary Report Features, Alert Totals

Feature	Description
State	Host/service status value. The row All States provides totals of each type of alert for all possible status values.
Soft Alerts	Number of SOFT alerts for the given status value – see *Hard and Soft Status Condition Definitions*, page 1-7
Hard Alerts	Number of HARD alerts for the given status value
Total Alerts	Total number of alerts (SOFT + HARD) for the given status value

The following table describes the features specific to Alert Summary reports of type Top Alert Producers. For a description of the fields common to all Alert Summary reports, see *Alert Summary Report Features, General*, page 2-69.

Table 2-71: Alert Summary Report Features, Top Alert Producers

Feature	Description
Rank	Higher rank is indicated by a smaller number, and means more alerts produced.
Producer Type	Whether a host or service alert
Host	Name of the host Click the host name to display the Host Information view – see *Host Information*, page 2-103.

Table 2-71: Alert Summary Report Features, Top Alert Producers (Continued)

Feature	Description
Service	Name of the service
	Click the service name to display the Service Information view – see *Service Information*, page 2-106.
Total Alerts	Number of alerts produced by the alert producer

Table 2-72: Links **To** the Alert Summary View

Origin	Link
left menu	Alert Summary

Table 2-73: Links **From** the Alert Summary View

Destination	Link
Host Information, page 2-103	host
Service Information, page 2-106	service

Notifications

The Notifications view provides a chronology of the host and service notifications that have been sent to the system contact. It shows notifications for a specific host, a specific service, or all hosts and services, depending on how the view is accessed.

The Notifications view lets you see what notifications were sent, when. Notifications are sent whenever host or service problems are detected or resolved. You can filter this view to display only notifications of a specific type, and you can display the notifications for any given day.

The following table describes the Notifications view features.

Table 2-74: Notifications View Features

Feature	Description
Log File Navigation	Day covered by the current view
	Click the left (right) arrow to view notifications from the previous (next) day.
Host	Origin of the notification (corresponds to the Host field of the notification email)
	Click the link for details – see *Host Information*, page 2-103.
Service	Origin of the notification (corresponds to the Service field of the notification email). Service is N/A ("not available") if host is down.
	Click the link for details – see *Service Information*, page 2-106.
Type	Notification type, color coded (corresponds to the Notification Type field of the notification email). Blue: information, green: normal, yellow: warning, red: failure, orange: unknown. Examples: HOST DOWN, CRITICAL, ACKNOWLEDGEMENT
Time	Date and time the notification was sent (corresponds to the Date/Time field of the notification email)
Contact	Notification contact name: the administrator account, persistadmin
	Click the persistadmin contact link for details – see Contacts, *View Config*, page 2-94.
Notification Command	Notification command name (defined during system configuration)
	Click the link for details – see Commands, *View Config*, page 2-94.
Information	Additional information (corresponds to the Additional Info field of the notification email)
update form (upper right)	To update the Notifications view – 1.Choose the following update options: – To show only certain types of notification, choose a notification type in the pulldown list Notification detail level. – To change the notification list order, click the check box Older Entries First. 2.Click Update.

See Also

- *View Config*, page 2-94, for object types Hosts, Services, and Contacts; describes the host and service status values that cause notifications to be sent.

Related Views

- The information in the Notifications view is a subset of that in the Event Log view – see *Event Log*, page 2-74.

Table 2-75: Links **To** the Notifications View

Origin	**Link**
left menu	Notifications
Service Detail, page 2-26, when main heading is Service Status Details For All Hosts	View Notifications For All Hosts
Service Problems, page 2-34	View Notifications For All Hosts
Alert History, page 2-64 • for all hosts and services • single host • single service	View Notifications For: • All Hosts • This Host • This Service
Trends, page 2-51	View Notifications For This Host/Service
Availability, page 2-55, for single host or service	View Notifications For This Host/Service
Alert Histogram, page 2-60	View Notifications For This Host/Service
Host Information, page 2-103	View Notifications For This Host
Service Information, page 2-106	View Notifications For This Service

Table 2-76: Links **From** the Notifications View

Destination	**Link**
When main view heading is All Hosts and Services	
Service Detail, page 2-26	View Status Detail For All Hosts
Alert History, page 2-64	View History For All Hosts

Table 2-76: Links **From** the Notifications View (Continued)

Destination	Link
When view shows notifications for a single host or service	
Alert History, page 2-64, for this host/service	View History For This Host/Service
Trends, page 2-51, for this host/service	View Trends For This Host/Service
When view shows notifications for a single host	
Service Detail, page 2-26, for this host	View Status Detail For This Host
When the main view heading is All Contacts **and the view shows notifications**	
Host Information, page 2-103	specific host name
Service Information, page 2-106	specific service name

Event Log

The Event Log view provides a chronology of logged PCC events.

The Nagios event log (file `/var/log/nagios/nagios.log`) is rotated daily at midnight, and a copy named with the date (for example, `nagios-12-20-2002-00.log`) is placed in the archive directory, `/var/log/nagios/archives`.

The following table describes the Event Log view features.

Table 2-77: Event Log View Features

Feature	Description
update form (upper right)	To update the Event Log view to change the event list order, click the check box Older Entries First, and then click Update.
Log File Navigation	Day covered by the current view
	Click the left (right) arrow to view events from the previous (next) day.

Table 2-77: Event Log View Features (Continued)

Feature	Description
events	The information for an event includes information such as the following (not all event types include all of the information): • Color-coded status icon (blue: information, green: normal, yellow: warning, red: failure, orange: unknown) • Time stamp • Event type: HOST or SERVICE • Host identifier • Service identifier (service alerts only) • Host or service status value – see *Host and Service Status Value Definitions*, page 1-6 • Status condition (HARD or SOFT) – see *Hard and Soft Status Condition Definitions*, page 1-7 • Sequential identifier for this event message – indicates how many times it has been sent • Event message: additional information describing the event

Related Views

- The information in the Alert History view is a subset of that in the Event Log view – see *Alert History*, page 2-64.
- *Alert Histogram*, page 2-60, shows the number of alerts of different types for hosts and/or services.
- *Trends*, page 2-51, shows status value trends over time for hosts and/or services.

Table 2-78: Links **To** the Event Log View

Origin	Link
left menu	Event Log

Links *from* the Event Log view: none.

Application Manager

The Application Manager view provides the ability to start, stop, and restart one or more servers on the system. Use this view only when necessary, such as when upgrading a host or before a planned power outage. This view should be used only by service personnel or administrators.

The features of the Application Manager view are described in the following table.

Table 2-79: Application Manager Features

Feature	Description
server group title	Name of the server group currently shown in this view: • ALL Systems – All server groups. • MINING Servers – All email mining servers. • HTTP Servers – All HTTP portal servers. • SMTP Servers – All SMTP portal servers. • META Servers – All metaservers. • SMARTCELLS Servers – All smart cell servers.
Number	If ALL Systems are displayed: • Number of server groups found in the system. If a specific server group is displayed: • Number of hosts in a specific group.
Group Selection	Click one of the buttons to select all server groups or a specific server group to affect: • ALL Systems • MINING Servers • HTTP Servers • SMTP Servers • META Servers • SMARTCELLS PCC Servers and DB2 Servers are not available buttons because you should not perform actions on these servers separately. You must perform actions on these servers in a specific order, which you can perform only when performing an action on ALL Systems.

Table 2-79: Application Manager Features (Continued)

Feature	Description
Action	Click the button to perform the indicated action: • Start – Start all systems or all the hosts in the selected server group. • Stop – Stop all systems or all the hosts in the selected server group. • Restart – Stop and immediately start all systems or all the hosts in the selected server group.
Status Area	Shows the status of the action performed.
All Systems	If ALL Systems are displayed, shows all the server groups associated with the system. • General status of the server group. A check icon () indicates normal operation. An X icon () indicates one or more servers in that group is down. An ! icon () indicates an action is pending. • Group name: – META Servers – SMARTCELLS Servers – MINING Servers – HTTP Servers – SMTP Servers – PCC Servers – DB2 Servers • Number of servers in the group. • Group status (STARTED, STOPPED, STARTING, STOPPING, and PENDING).
Server Group	If a specific server group is displayed, shows all the hosts in the group. • General status of the host. A check icon () indicates normal operation. An X icon () indicates one or more servers in that group is down. • Host name. • IP address. • Host status (STARTED, STOPPED, STARTING, STOPPING, and PENDING).

Table 2-80: Links **To** the Application Manager View

Origin	Link
left menu	Application Manager

Links from the Application Manager view: none.

Replication

You use the Replication view to monitor and start or stop replicating a domain on a remote system. Replication status is updated after each polling cycle, so it could be up to 5 minutes after you start replication before you see the results on the graph of replication rates. Errors and warnings, however, are displayed as soon as they happen on the system. (The Replication view is unavailable until at least one domain on the PCC host system is configured for replication.)

The failure of a replicated smart cell triggers the allocation of new primary and secondary smart cells on the replica site. When the original site returns to service, it automatically becomes the replica site for the new primary and secondary smart cells. Depending on the configuration, some administration may be necessary for continued data storage. Specifically, if the system uses Email Mining, the replica site mining servers must be configured and enabled to start mining to the replica site.

If the primary site is not available for queries, end-users must enter the address of the replica site, instead of the primary site, in their browsers.

The features of the Replication view are described in the following table.

Table 2-81: Replication View Features

Feature	Description
Domain Information	For each domain that is configured for replication: • Domain Name – the DNS name of the domain • Service – whether replication is in progress (Running) or not (Stopped) • Between – the names of the local and replication systems. The first system named is the location of the domain. The second system named is the remote system, where the domain is being replicated. • Current Transfer Rate – how many messages and documents are being duplicated per second • Current Percentage of Data Replicated – how much of the data currently stored in the domain has been duplicated
	Click the Details button to view replication status for each group in the domain and replication performance over various periods. For each group in the domain, the detail view shows: • Status, name, and total messages of the group on the local system. A check icon () indicates normal operation. An X icon () indicates that replication failed the last time it was tried, and the ! icon () indicates that replication is being retried. • An arrow showing the direction of the data between the groups. Normally, the direction is left to right, from the group on the local host to the group on the remote host. In a failover situation, the direction is right to left, as data replicated on the remote host is being used to restore the group on the local host. • Name and total messages of the replication group • How much of the data in the source group has been copied to the destination group A graph shows the number of messages stored per second on the local and replication (remote) systems for the selected domain. You can select the last year, last month, last 24 hours, or last hour to graph.

Table 2-81: Replication View Features (Continued)

Feature	Description
Action	Click the available button below the domain information to perform the indicated action: • START NOW – Start replicating the specified domain. Replication will replicate the batch that was next when it stopped. • STOP NOW – Stop replicating the specified domain. Replication will stop after the current batch is prerlicated.

Related Views

- *View Cell Space*, page 2-24
- *SmartCell Cloning*, page 2-91

Table 2-82: Links **To** the Replication View

Origin	Link
left menu	Replication

Links *from* the Replication view: none.

Email Mining

The Email Mining view provides status information about the mining system for each domain. It shows information about the Exchange server, mining server, and system as well as mining system information about the host and service status. In addition, this view provides graphical store rate information. If email mining is not available or running, an error message is displayed.

The features of the Email Mining view are described in the following table.

Table 2-83: Email Mining View Features

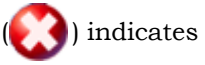
Feature	Description
Exchange Server	Information about the Exchange server and its status. For servers with more than one domain, choose a domain from the pulldown list. For each domain: • Server host name or IP address • General status of the Exchange server. A check icon () indicates normal operation. An X icon () indicates a problem or inactive service. • Name and size of the mailbox • Number of items
Mining Server	Information about the mining server and its status. • Server host name or IP address • General status of the mining server. A check icon () indicates normal operation. An X icon () indicates a problem. An ! icon () indicates mining has stopped. • Number of journal and email miners • Rate and number of stored journal items • Number of rejected items • Number of stubs created. A stub is a representation of the original email that has been mined. • Number of stored email items

Table 2-83: Email Mining View Features (Continued)

Feature	Description
Appliance	Information about RISS and its status. • Server host name or IP address • General status of the system. A check icon () indicates normal operation. An X icon () or ! icon () indicates a problem or inactive service. • Domain names • Rate and number of stored items • Number of SMTP portals
Action	Click the available button below the server information to perform the indicated action: • STOP NOW – Stop the mining server. • START NOW – Start the mining server. Based on the number of servers, there is a latency period when stopping or starting the servers.
Mining System Info	Host and service status information about the mining system. • Host name and IP address • Host sending mode. INTERNAL is the default and indicates data is being sent directly to the RISS. EXTERNAL indicates data is being sent to memory before reaching the RISS. RELAY indicates a mix of internal and external sending modes are occurring. UNKNOWN indicates a potential problem. • Status of Jboss, Mail Attender, and Miner Manager services. • Status of journal and mailbox TNEF services (ON or OFF).
Historical Store Rate graph	Graphs the number of messages per second each domain on the system has stored given a specified time frame. The default shows the storage rate in the last hour, ending with the current time. Click Last 24 Hours, Last Month, or Last Year to change the time period.

Table 2-84: Links **To** the Email Mining View

Origin	Link
left menu	Email Mining

Links from the Email Mining view: none.

User Manager

The User Manager view lets you configure Dynamic Account Synchronization (DAS) to automatically create and update email user accounts on RISS. You can define multiple configurations to extract various sets of users from one or more LDAP servers for specific RISS domains.

How to Configure DAS

Items in the User Manager view are links to steps in the configuration process. Click the links as follows to define a DAS configuration:

1. Click LDAP Servers to set up a connection to an LDAP server.
2. Click Configurations to name the DAS configuration and link it to the LDAP connection that you set up in step 1.
3. Click Mappings to specify, for the selected configuration, where DAS will extract users in the LDAP tree and where it will add or update users on RISS.
4. Click Assignments to specify where and when the selected DAS configuration will be run.

Configuration details are described with their links in the following sub-sections.

Configurations

The Configurations link in the User Manager view lets you create a configuration and associate it with a defined server connection. You can also delete and view configurations from this link. The features of the Configurations view are described in the following table.

Table 2-85: User Manager View, Configurations Features

Feature	Description
Create	1. Click Create to specify a new configuration. The New Configuration name box is displayed. 2. Enter a name to identify this configuration. Do not use spaces. 3. Click Add to create the configuration. 4. Click Back to return to Configurations and associate the configuration with an LDAP server connection. If you have not yet created the LDAP server connection, click Back to main to return to the User Manager view.
List of selectable configurations	Select an existing DAS configuration to delete or associate with an LDAP server. If you just created a configuration, select it and click the Server button.
Actions	Click a button to perform one of the following actions on a selected DAS configuration: • Delete – Delete the configuration. • Server – Create, view, or change the associated LDAP server. A new view displays pulldown lists of available DAS configurations and server connections. (Server connections are created using LDAP Servers in the User Manager view.) – Select the desired configuration and the server connection. Multiple DAS configurations can be associated with the same server connection. – Click the Associate button. – Click Back to return to the Configurations, or click Back to main to return to the User Manager view.
	Click Back to refresh the Configurations view. Click Back to main to return to the User Manager view.

LDAP Servers

The LDAP Servers link in the User Manager view lets you define, update, or delete a connection to an LDAP server. LDAP server connections include all the information that DAS needs to access an LDAP server.

Table 2-86: User Manager View, LDAP Servers Features

Feature	Description
List of selectable LDAP server connections	Select an existing LDAP server connection to update or delete.
Actions	Click a button to perform one of the following actions on a selected LDAP server connection: • Update – Change the connection. A new view displays the current host, port, user, and password. – Click Reset if you want to clear all values. – Enter new values as needed. – Click Update to save your changes. – Click Back to return to LDAP Servers, or click Back to main to return to the User Manager view. • Delete – Remove the connection.
Create	1. Click Create to define a new LDAP server connection. 2. Enter the following values: – Server ID – A name to identify the server connection; for example, "server250" for the LDAP server 1.1.1.250. The name must be unique among other server connections on the system. – Hostname – The IP address of the LDAP server where the desired user information is located. – Port – The LDAP server port that DAS will use. The default is 389. – Binder user – A user ID that has at least read access to user accounts on the LDAP server. You may want to create a user profile on the LDAP server specifically for DAS use. Include the domain in this entry; for example, for a user named dasUser and the domain `ldaptest.com`, you would enter cn=dasUser,cn=Users,dc=ldaptest,dc=com.The default user ID is Administrator (cn=Administrator,cn=Users,dc=ldaptest,dc=com). – Binder pswd – The password associated with the binder user. 3. Click Create to save the defined server connection. The system attempts to validate the connection. 4. Click Back to return to LDAP servers, or click Back to main to return to the User Manager view.

Table 2-86: User Manager View, LDAP Servers Features (Continued)

Feature	Description
Other actions	Click Back to refresh the LDAP servers view. Click Back to main to return to the User Manager view.

DAS Mappings

The DAS Mappings link in the User Manager view lets you create, view, or delete DAS configuration specifications of the users to be monitored on the LDAP server and the users to be sychronized on RISS. A DAS configuration can have only one such mapping. Features of the DAS Mappings view are described in the following table.

Table 2-87: User Manager View, DAS Mappings Features

Feature	Description
Create	1. Click Create to specify a new configuration. A mapping entry form is displayed, or a message informs you that there are no configurations to be mapped. 2. Enter the desired value for each parameter in the mapping entry form (described in the following rows). 3. Click Update to save your entries. 4. Click Back to main to return to the User Manager view and assign the DAS configuration to a DAS service, or click Back to return to DAS Mappings.
Current DAS Mappings	The current mapping values for all mapped DAS configurations. You can change the values or delete the entire mapping in this view. Mapping values are described in the following rows.
• Configuration ID	The DAS configuration that uses this mapping. Select the desired configuration from the pulldown list. (Use the Configurations link to create a configuration.)
• Source LDAP Domain name	The domain on the LDAP server where user accounts are to be monitored; for example, `ldaptest.com`
• Starting Point	The root node where user accounts are stored on the LDAP server. For example, enter cn=Users,dc=ldaptest,dc=com for the node `Users` in the domain `ldaptest.com`.. The value must specify the relative location in the LDAP tree, including parent nodes and the domain name.

Table 2-87: User Manager View, DAS Mappings Features (Continued)

Feature	Description
• Group Name	(for future use)
• Update LDAP filter	Criteria to include or exclude specific users. HP recommends that you use at least the default value, "(objectclass=user)(mail=*)," which excludes users that do not have email accounts.
• USNChanged	Active Directory's unique sequence number (USN) the last time DAS ran. Active Directory increments the USN for each change in any of its user accounts. When DAS finds a larger USN, it extracts the new information. For the initial RISS setup, set USNChanged to "1" so that DAS extracts all users. Thereafter, do not change this value. *You must stop all scheduled jobs for this DAS configuration to change* USNChanged*. Use the* Configuration Command Panel *in the* Assignment *view (see Assignment, page 2-88).*
• Target appliance Domain ID	The ID (not the name) of the RISS domain where users are synchronized with users on the LDAP server.
• Default Password	A default password that is assigned to all new users that are added when this DAS configuration is run.
• NextRepID	The RISS repository ID that is assigned to new users. DAS retrieves this value from the database, but you can use this feature to specify the repository ID for the first user that is inserted when DAS runs. For example, if you enter 67, the repository that is created and assigned for the first imported user will be R0000067. You can use this feature if users already exist in the system or you want to reserve repository IDs for any reason. If you specify a value that is lower than an existing repository ID, DAS will automatically correct the value to the next higher number. *You must stop all scheduled DAS configurations that import users to the domain that the specified repository belongs to if you want to change* NextRepID*. Use the* Configuration Command Panel *in the* Assignment *view (see Assignment,* page 2-88*).*

Table 2-87: User Manager View, DAS Mappings Features (Continued)

Feature	Description
• DeleteStartingPoint	The root node where deleted user objects are stored on the LDAP server. For example, enter cn=deletedObjects,dc=ldaptest,dc=com for the node `deletedobjects` in the domain `ldaptest.com`.. The value must specify the relative location in the LDAP tree, including parent nodes and the domain name.
• Delete LDAP Filter	Criteria to include or exclude specific users in the LDAP deleted users directory. Add to the default for special cases.
• Delete USNChanged	The USN in the deleted users directory the last time DAS ran. For the initial RISS setup, set this value to "0". Thereafter, do not change this value. *You must stop all scheduled jobs for this DAS configuration to change the* Delete USNChanged. *Use the* Configuration Command Panel *in the* Assignment *view (see Assignment, page 2-88).*
Actions	Click a button to perform one of the following actions on the DAS mapping immediately above the button: • Update – Save any new values you entered for mapping parameters. • Delete – Remove the mapping.
	Click Back to main to return to the User Manager view.

Assignment

The Assignment link in the User Manager view lets you assign a DAS configuration to a DAS server and start or schedule DAS jobs. Features of the Assignment view are described in the following table.

Table 2-88: User Manager View, Assignment Features

Feature	Description
Create	1. Click Create to specify a new assignment. An entry form is displayed. 2. Enter the following values: – ConfigID – The DAS configuration that is to be run on the portal (specified below). Select the configuration from the pulldown list. (Use the Configurations link to create a configuration.) – DAS Server IP – The IP address of the HTTP portal where the DAS service runs the selected DAS configuration. – Configuration Enabled – Whether or not the selected DAS configuration is available to be run. To finish a new assignment, select Yes so that you can run the service and set up necessary database and configuration files (see steps 4 and 5). – Configuration running state – (for future use) – Period (mn) – The number of minutes between runs of the selected DAS configuration. A period of 0 means the job will run once. – DAS server running state – (for future use) 3. Click Update to save your entries. 4. In the Configuration Command Panel, select Yes for Initialize DAS setup. (Select Yes only when you are scheduling or starting the DAS configuration for the first time, or if you need to resynchronize the database in recovery from an unusual event.) 5. Click Start to run the DAS configuration immediately. 6. Click Back to main to return to the User Manager view, or click Back to return to Assignment. 7. When DAS has updated the database, return to the Assignment view and change the configuration as follows: – In the Configuration Command Panel, select No for Initialize DAS setup. – Click Schedule to run the DAS configuration periodically (as specified in step 2). *Leaving* Initialize DAS setup *set to* Yes *after the first run prevents DAS from properly updating RISS user accounts.*

Table 2-88: User Manager View, Assignment Features (Continued)

Feature	Description
Current Assignments	The current assignments of all assigned DAS configurations. You can change the values or delete the entire assignment in this view.
Actions	Click a button to perform one of the following actions on the assignment immediately above the button: • Update – Save any new assignment values you entered. • Delete – Remove the assignment for the selected DAS configuration.
Configuration Command Panel	Run commands for the DAS configuration whose assignment is displayed immediately above the panel. • Initialize DAS setup – Whether or not DAS creates database and configuration files when it runs. Select No after the first run of this configuration. *Leaving* Initialize DAS setup *set to* Yes *after the first run prevents DAS from properly updating RISS user accounts.* • Start – Run the configuration immediately. • Schedule – Run the configuration periodically, as specified in the assignment values. • Stop – Cease running the configuration. • Remove config files – Delete the configuration files that DAS created for this configuration.
DAS Server Command Panel	Run commands for the DAS service that is specified in the assignment immediately above the panel. • StartDASServer – Start the DAS service on the specified HTTP portal. All configurations that are enabled and assigned to this portal will run on schedule. • StopDASServer – Stop the DAS service on the specified HTTP portal. When the service is stopped, all scheduled configurations that are assigned to the portal are stopped.
Other Actions	Click Back to main to return to the User Manager view.

Portal Servers (https)

The Portal Servers (https) link on the User Manager view lists HTTP servers with their assigned DAS configurations.

Table 2-89: User Manager View, Portal Servers (https) Features

Feature	Description
List of servers	All HTTP portals in the system that hosts this PCC. Assigned DAS configurations are listed under each portal.
	Click a DAS configuration to move to the Assignment view, where you can view, change, delete, or start and stop the configuration.

Table 2-90: Links **To** the User Manager View

Origin	Link
left menu	User Manager

Links from the User Manager view: none.

See Also

- *User Accounts and PAM*, page 3-2.

SmartCell Cloning

The SmartCell Cloning view shows the status of current and past cloning operations and lets you clone a smart cell. You can clone a smart cell if its mirror smart cell is SUSPENDED, DEAD, or FAILED. (See *Smart Cell Life Cycle State Definitions*, page 1-4.)

Cloning a smart cell copies all of its information to another smart cell that is in the FREE state, in order to give the smart cell a new, viable mirror. The cloning operation can take a long time (even a day) depending on the amount of information to be cloned.

When you enter the SmartCell Cloning view, PCC searches for ongoing cloning operations and loads current data. Only one smart cell can be cloned at a time, so you will see the progress of any ongoing cloning operation.

The features of the SmartCell Cloning view are described in the following table.

Table 2-91: SmartCell Cloning View Features

Feature	Description
Cloning Set up	Lists any smart cells whose mirrors are not viable and shows you how many free cells are available. • Source – The IP address of a smart cell without a viable mirror. If all smart cells have viable mirrors, the view displays "No Broken Groups Found." If more than one smart cell needs a mirror, a Change Source button is present below the automatically selected IP address. • Free Cells – The number of smart cells that are currently in the FREE state. This is decremented by one after a cloning operation starts. Click the Change Source button, when present, to select a different smart cell for cloning. When the selection box appears, select the desired smart cell from the pull-down list and click the Select button.
Clone Cell	Click the Clone Cell button to start cloning the selected source. This button is unavailable if there are no smart cells to clone.
Status Area	Shows the following information about an ongoing cloning operation: • Source selected – The IP address of the smart cell that is being duplicated • Target selected – The IP address of the smart cell that is receiving the duplicate data • Current Step Percentage – A dynamic bar showing how much of the source data has been duplicated • Overall Percentage – The current step in the cloning operation. The steps are Initializing, Assigning target host, Transferring data, Transferring indexes, Waiting for indexer to complete, Updating history log, and Completed or Failed. Some steps happen so quickly that you may not see them. Steps such as Transferring data and Transferring indexes can take a long time if there is much data to clone. The check icon () indicates that the cloning operation is proceeding normally. If the operation fails, an X icon () is displayed.

Table 2-91: SmartCell Cloning View Features (Continued)

Feature	Description
History Logs	Shows the following information about each cloning operation that has occurred since startup: • Source • Target • Time Elapsed • Status • Date

Table 2-92: Links **To** the SmartCell Cloning View

Origin	Link
left menu	SmartCell Cloning

Links from the SmartCell Cloning view: none.

See Also

- *Smart Cell Life Cycle State Definitions*, page 1-4.

Update PCC

The Update PCC left menu item refreshes PCC views to reflect changes in the system configuration. For example, if you add a new smart cell or SMTP portal machine, you can use this menu item to view the effect in the Status Summary view. A pop-up (Done Refreshing Now) lets you know when the update is complete.

Links to and from the Update PCC view: none.

See Also

- *Status Summary*, page 2-11.

Software Versions

The Software Versions view shows the software versions of the hosts in each host group. You choose the host group using the HostType pulldown list at the upper right. Alternatively, you can choose System as HostType to display all the software versions of machines in the system.

The features of the Software Versions view are described in the following table.

Table 2-93: Software Versions Features

Feature	Description
Host Name	IP address of the host. (Not available for HostType System.)
Core Version	Versions of RISS software used. This software includes the operating system.
Application Version	Versions of RISS software used.
Installer Version	Versions of the software used to install the system.
Patches Applied	History of patches that were applied to the system.

Links to and from the Software Versions view: none.

View Config

The View Config view shows the system configuration from different points of view, based on different object types. It lets you examine *system parameters* as defined when the system was configured. It does *not* let you *change* any parameters; it is read-only.

The View Config view always shows RISS settings made at the time of system configuration/installation. This means that even though you can dynamically change some of the parameters displayed in the View Config view, using other PCC views (for example, enabling/disabling host checking), the View Config values do *not* reflect these changes.

You choose the type of object to display, using the Object Type pulldown list at the upper right. The tables below describe the different configuration displays.

Table 2-94: View Config View Features, Hosts

Feature	Description
Host Name	Name of the host. Example: sc-s2-204-4.
Alias/ Description	Long name or description of the host. Example: SmartCellMachines:sc-s2-204-4.ourcompany.com.
Address	IP address of the host. Example: 10.0.204.4
Parent Hosts	Parents of the host. Example: cr-s0-96-4, cr-s0-96-3. *Note:* The only RISS hosts that have parent hosts are the HTTP portals and the smart cells (the cloud routers are their parents).
Notification Interval	This is always No Renotification, meaning only one notification is sent when a host is detected as having a problem (see next).
Notification Options	The host status values that can cause a notification to be sent: DOWN, UNREACHABLE, and RECOVERY, where RECOVERY represents a transition from a problem status value (DOWN or UNREACHABLE) to the normal status value (UP).
Notification Period	Name of the defined notification period: always. The always value means notifications can be sent at any time; they are sent immediately. Click the link to display the definition of the always period – see *View Config View Features, Time Periods*, page 2-99.
Max. Check Attempts	Maximum number of times to check this host before a host problem status condition is considered HARD. See *Hard and Soft Status Condition Definitions*, page 1-7, for definitions of status conditions.
Host Check Command	The command used to check this host. Click the link to display the command definition – see *View Config View Features, Commands*, page 2-99.
Enable Checks	Whether or not host checking is currently enabled.
Retention Options	The types of information that are retained in the retention file, `/usr/local/nagios/var/status.sav`: all types of information.

Table 2-94: View Config View Features, Hosts (Continued)

Feature	Description
(*Not used* by the PCC: Event Handler, Enable Event Handler, Stalking Options, Enable Flap Detection, Low Flap Threshold, High Flap Threshold, Process Performance Data, Enable Failure Prediction, and Failure Prediction Options.)	

Table 2-95: View Config View Features, Host Groups

Feature	Description
Group Name	Name of the host group. Example: sc.
Description	Description of the host group. Example: SmartCellMachines:sc-s2-204-4.ourcompany.com.
Default Contact Groups	Contact groups defined for the host group: allAdmins is the only contact group used by the PCC.
	Click the contact group link to display the definition of the contact group – see *View Config View Features, Contact Groups*, page 2-99.
Host Members	All hosts in the host group.
	Click a host link to display the configuration information for the host – see *View Config View Features, Hosts*, page 2-95.

Table 2-96: View Config View Features, Services

Feature	Description
Host	Name of the host on which the service is running.
	Click the link to display the configuration information for the host – see *View Config View Features, Hosts*, page 2-95.
Description	Description of the service. Example: Spine Check.
Max. Check Attempts	Maximum number of times to check this service, before a service problem status condition is considered HARD – see *Hard and Soft Status Condition Definitions*, page 1-7.
Normal Check Interval	The time between ordinary checks of the service.
Retry Check Interval	The time between checks of the service when it is not responding.

Table 2-96: View Config View Features, Services (Continued)

Feature	Description
Check Command	The command used to check this service.
	Click the link to display the command definition – see *View Config View Features, Commands*, page 2-99.
Check Period	Name of the defined checking period: always. The always value means the service can be checked at any time.
	Click the link to display the definition of the always period – see *View Config View Features, Time Periods*, page 2-99.
Enable Active Checks	Whether or not active service checks are currently enabled.
Default Contact Groups	Contact groups defined for the service: allAdmins is the only contact group used by the PCC.
	Click a contact group link to display the definition of the contact group – see *View Config View Features, Contact Groups*, page 2-99.
Enable Notifications	Whether or not notifications are currently enabled for this service.
Notification Interval	This is always No Renotification, meaning only one notification is sent when a service is detected as having a problem (see next).
Notification Options	The service status values that can cause a notification to be sent: CRITICAL and RECOVERY, where RECOVERY represents a transition from a CRITICAL status value to the normal status value (OK).
Notification Period	Name of the defined notification period: always. The always value means notifications can be sent at any time; they are sent immediately.
	Click the link to display the definition of the always period – see *View Config View Features, Time Periods*, page 2-99.
Retention Options	The types of information that are retained in the retention file, `/usr/local/nagios/var/status.sav`: all types of information.
(*Not used* by PCC: Parallelize, Volatile, Obsess Over, Enable Passive Checks, Check Freshness, Freshness Threshold, Event Handler, Enable Event Handler, Stalking Options, Enable Flap Detection, Low Flap Threshold, High Flap Threshold, Process Performance Data, Enable Failure Prediction, and Failure Prediction Options.)	

Table 2-97: View Config View Features, Contacts

Feature	Description
Contact Name	Name of the contact: persistadmin is the only contact used by PCC.
Alias	Long name of the contact: Administrator.
Email Address	Email address for the contact: `bogus@persistcorp.com`. Defined for the system at configuration time. *Note:* This can be a comma-separated list of email addresses. In that case, what is defined as the contact (a single contact, *not* a contact group – see *View Config View Features, Contact Groups*, page 2-99) represents more than one email destination.
	Click the link to compose and mail a new message to the contact.
Pager Address/ Number	*Not used* by PCC.
Service Notification Options	The service status values that cause a notification to be sent to the contact: CRITICAL and RECOVERY, where RECOVERY represents a transition from a CRITICAL status value to the normal status value (OK).
Host Notification Options	The host status values that cause a notification to be sent to the contact: DOWN, and RECOVERY, where RECOVERY represents a transition from a problem status value (DOWN or UNREACHABLE) to the normal status value (UP).
Service Notification Period	Name of the defined notification period: always. The always value means notifications can be sent at any time; they are sent immediately.
	Click the link to display the definition of the always period – see *View Config View Features, Time Periods*, page 2-99.
Host Notification Period	Name of the defined notification period: always. The always value means notifications can be sent at any time; they are sent immediately.
	Click the link to display the definition of the always period – see *View Config View Features, Time Periods*, page 2-99.
Service Notification Commands	Names of the defined notification commands for services.
	Click a link to display the definition of the command – see *View Config View Features, Commands*, page 2-99.

Table 2-97: View Config View Features, Contacts (Continued)

Feature	Description
Host Notification Commands	Names of the defined notification commands for hosts.
	Click a link to display the definition of the command – see *View Config View Features, Commands*, page 2-99.

Table 2-98: View Config View Features, Contact Groups

Feature	Description
Group Name	Name of the contact group: allAdmins is the only contact group used by PCC.
Description	Description of the contact group: All system administrators.
Contact Members	Names of all contacts in the contact group: persistadmin is the only contact used by PCC.
	Click the persistadmin contact link to display the definition of the contact – see *View Config View Features, Contacts*, page 2-98.

Table 2-99: View Config View Features, **Time Periods**

Feature	Description
Name	Name of the defined time period: always.
Alias/Description	Long name or description of the time period: alwaysContactMe.
<day of week> Time Ranges	Time period defined for the given day of the week. The always time period has no time restriction on any day of the week.

Table 2-100: View Config View Features, Commands

Feature	Description
Command Name	Name of the command. Example: check_ping.
Command Line	The command itself (its definition). Example: $USER1$/check_ping -H $HOSTADDRESS$ -w 200.0,20% -c 1000.0,60% -p 5.

Table 2-101: Links **To** the View Config View

Origin	Link
left menu	View Config
Notifications, page 2-71	• persistadmin contact (Contacts display) • specific command (Commands display)

Links *from* the View Config view: none.

Hostgroup Information

The Hostgroup Information view provides information on the performance of service monitoring for a given host group. Except for the addition of access to Hostgroup Commands, this view provides the same information as that in the Nagios Stats view, filtered for a single host group.

The following table describes the Hostgroup Information view features.

Table 2-102: Hostgroup Information View Features

Feature	Description
Time Frame/ Checks Completed	The number and percentage of PCC services checked in the indicated time frames (since PCC startup or in the last 1, 5, 15, or 60 minutes).
Check Metric/Min/Max/Average • Execution Time • Latency	The minimum, maximum and average times: • it took to check a service • between the time a service check was scheduled and the time it was executed (% State Change is *not used* by PCC.)

Table 2-102: Hostgroup Information View Features (Continued)

Feature	Description
Hostgroup Commands	To run a command to perform an action on this host group, click the corresponding command link. This displays the External Command Interface view for the command – see *External Command Interface*, page 2-114. *Note:* Commands that *disable* (notifications, status checks, and so on) *override* commands that enable. For example, suppose you disable service checks for a particular host group using the Hostgroup Information view (command Disable checks of all services in this hostgroup), but you enable checks for all services using the Nagios Info view (command Start executing service checks). Services for the host group are *not* checked, because disabling overrides enabling.

The Passive Service Checks charts are *not used*; all PCC service checks are active.

Related Views

- For information on global commands that affect all host groups, see *Nagios Info*, page 2-39.
- The Nagios Stats view, presents the same monitoring performance information, but for all host groups; and it does not have Hostgroup Commands. See *Nagios Stats*, page 2-42.
- *Tactical Overview*, page 2-21, also provides (limited) information on monitoring performance.

Table 2-103: Links **To** the Hostgroup Information View

Origin	Link
Status Summary, page 2-11	host group abbreviation, in parentheses – example: (sc).
Status Overview, page 2-32	host group abbreviation, in parentheses – example: (sc).
Status Grid, page 2-108	host group abbreviation, in parentheses – example: (sc).

Table 2-104: Links **From** the Hostgroup Information View

Destination	Link
Service Detail, page 2-26, for this host group.	View Status Detail For This Hostgroup
Status Overview, page 2-32, for this host group.	View Status Overview For This Hostgroup
Status Grid, page 2-108, for this host group.	View Status Grid For This Hostgroup
Availability, page 2-55, for this host group.	View Availability For This Hostgroup
External Command Interface, page 2-114	specific Hostgroup Commands

Exceptions Stack-trace

The Exceptions Stack-trace view displays a program stack trace for each exception occurring on each host in a given host group.

Note: For monitoring purposes you normally do *not* need to use this view. It is intended for troubleshooting and configuration only by installers and advanced system administrators.

Table 2-105: Links **To** the Exceptions Stack-trace View

Origin	Link
System Status, page 2-14	host group name and number of exceptions, in the Exceptions chart – example: Smtp (2).

Table 2-106: Links **From** the Exceptions Stack-trace View

Destination	Link
System Status, page 2-14	Return to Summary

Host Information

The Host Information view provides status information for a given host, as described in the following table.

Table 2-107: Host Information View Features

Feature	Description
heading	Full and abbreviated names of this host, as well as host IP address. For example: • SmartCellMachines:sc-s1-172-1.mycorp.com – Full host name • sc-s1-172-1 – Abbreviated host name • 10.0.172.1 – IP address • SmartCellMachines:1 – This is the first host in host group SmartCellMachines
Host State Statistics	The amount and percentage of time this host has had each host status value, and the total time. See *Host Status Value Definitions*, page 1-6.
Host Commands	To run a command to perform an action on this host, click the corresponding command link. This displays the External Command Interface view for the command – see *External Command Interface*, page 2-114. *Note:* Commands that *disable* (notifications, status checks, and so on) *override* commands that enable. For example, suppose you disable checks for all services on a particular host using the Host Information view (command Disable checks of all services on this host), but you enable checks for all services on all hosts using the Nagios Info view (command Start executing service checks). Services for the particular host are *not* checked, because disabling overrides enabling.

Table 2-107: Host Information View Features (Continued)

Feature	Description
Host Comments	All comments for this host. Comments are notes you make to yourself or other system administrators. The following information is shown for each comment: • Entry Time – Time that the comment was added. • Author – Who entered the comment. • Comment – The comment text. • Comment ID – Unique sequential identifier, incremented whenever a new comment is added. • Persistent – Yes. PCC comments are always persistent. • Actions – Click the wastebasket icon () to delete this comment. To add a new comment for this host, or delete all comments for this host, click the appropriate link. This displays the External Command Interface view, where you enter the new comment or confirm deletion – see *External Command Interface*, page 2-114.
Host State Information	Status information for this host: • Host Status; Status Information; Last Status Check – Current status value, with additional status information and time of last status check. • Host Checks Enabled? – Whether or not this host gets checked for status. You can change this with the associated host command (see Host Commands, above). • Last State Change; Current State Duration – Time of the latest status value change; how long this host has had the current status value. • Last Host Notification; Current Notification Number – Time and number of the latest notification from this host. • Host Notifications Enabled? – Whether or not notifications are currently enabled for this host. You can change this with the associated host command (see Host Commands, below). This is overridden by the global Enable/Disable Notifications command – see *Nagios Info*, page 2-39. • In Scheduled Downtime? – Whether or not the current time is scheduled downtime for this host. • Last Update – Time this host was last checked.

Related Views

- For information on global commands that affect *all* hosts, see *Nagios Info*, page 2-39.

- *Comments*, page 2-36.

Table 2-108: Links **To** the Host Information View

Origin	Link
Service Detail, page 2-26	specific host name
Service Problems, page 2-34	specific host name
Host Detail, page 2-30	specific host name
Status Overview, page 2-32	Actions icon View Extended Information For This Host ()
Scheduling Queue, page 2-43	specific host name
Alert Summary, page 2-66	specific host name
Notifications, page 2-71	specific host name
Status Grid, page 2-108	specific host name
Service Information, page 2-106	View Information For This Host

Table 2-109: Links **From** the Host Information View

Destination	Link
Service Detail, page 2-26, for this host	View Status Detail For This Host
Alert History, page 2-64, for this host	View Alert History For This Host
Trends, page 2-51, for this host, for the last 24 hours	View Trends For This Host
Alert Histogram, page 2-60, for this host	View Alert Histogram For This Host
Availability, page 2-55, for this host	View Availability Report For This Host
Notifications, page 2-71, for this host	View Notifications For This Host
External Command Interface, page 2-114	command (Host Commands)

Service Information

The Service Information view provides status information for a given service, as described in the following table.

Table 2-110: Service Information View Features

Feature	Description
heading	Name of the service. Full and abbreviated names of this host, as well as host IP address. See *Host Information*, page 2-103.
Service State Statistics	The amount and percentage of time this service has had each service status value; and the total time. See *Service Status Value Definitions*, page 1-7.
Service Commands	To run a command to perform an action on this service, click the corresponding command link. This displays the External Command Interface view for the command – see *External Command Interface*, page 2-114. *Note:* Commands that *disable* (notifications, status checks, and so on) *override* commands that enable. For example, suppose you disable checks for a particular service such as PING using the Service Information view (command Disable checks of this service), but you enable checks for all services using the Nagios Info view (command Start executing service checks). The particular service (PING) is *not* checked, because disabling overrides enabling.
Service Comments	All comments for this service. Comments are notes you make to yourself or other system administrators. The following information is shown for each comment: • Entry Time – Time that the comment was added. • Author – Who entered the comment. • Comment – The comment text. • Comment ID – Unique sequential identifier, incremented whenever a new comment is added. • Persistent – Yes. PCC comments are always persistent. • Actions – Click the wastebasket icon () to delete this comment. To add a new comment for this service, or delete all comments for this service, click the appropriate link. This displays the External Command Interface view, where you enter the new comment or confirm deletion – see *External Command Interface*, page 2-114.

Table 2-110: Service Information View Features (Continued)

Feature	Description
Service State Information	Status information for this service: • Current Status; Status Information – Current service status value; additional status information. • Last Check Time; Next Scheduled Active Check – Times of the latest and next scheduled status checks. • Current Attempt – Number of successful attempts, and total number of attempts, to check this service. • Latency – Time elapsed from when the latest service check was scheduled to when it was executed. • Check Duration – Duration of the latest status check. • Service Checks Enabled? – Whether or not this service gets checked for status. You can change this with the associated service command (see Service Commands, above). • Last State Change; Current State Duration – Time this service last changed status value; how long it has had the current status value. • Last Host Notification; Current Notification Number – Time and number of the latest notification from this service. • Service Notifications Enabled? – Whether or not notifications are currently enabled for this service. You can change this with the associated service command (see Service Commands, below). This is overridden by the global Enable/Disable Notifications command – see *Nagios Info*, page 2-39. • In Scheduled Downtime? – Whether or not the current time is scheduled downtime for the host of this service. • Last Update – Time this service was last checked. (Last Check Type, State Type and Percent State Change are *not used* by the PCC.)

Related Views

- For information on global commands that affect *all* services, see *Nagios Info*, page 2-39.
- *Comments*, page 2-36.

Table 2-111: Links **To** the Service Information View

Origin	Link
Service Detail, page 2-26	service name
Service Problems, page 2-34	service name
Scheduling Queue, page 2-43	service name
Alert Summary, page 2-66	service name
Notifications, page 2-71	service name
Status Grid, page 2-108	service name

Table 2-112: Links **From** the Service Information View

Destination	Link
Host Information, page 2-103	View Information For This Host
Service Detail, page 2-26, for this host	View Status Detail For This Host
Alert History, page 2-64, for this service	View Alert History For This Service
Trends, page 2-51, for this service, for the last 24 hours	View Trends For This Service
Alert Histogram, page 2-60, for this service	View Alert Histogram For This Service
Availability, page 2-55, for this service	View Availability Report For This Service
Notifications, page 2-71, for this service	View Notifications For This Service
External Command Interface, page 2-114	command (Service Commands)

Status Grid

The Status Grid view provides a high-level view of hosts and services, organized by host group. Each host and service is listed, and its status value is shown by color coding (see *Host and Service Status Value Definitions*, page 1-6). You can click a given host or service entry to see details.

The charts Host Status Totals and Service Status Totals of the Status Grid view are the same as those of the Status Summary view – see *Status Summary*, page 2-11.

The following table describes the Status Grid view features for a *single* host group.

Table 2-113: Status Grid View, Hostgroup Features

Feature	Description
host group	Host group name and abbreviation.
	Click a host group name, such as SmartCells, to display the Service Detail view for that host group. See *Service Detail*, page 2-26.
	Click the parenthetical abbreviation of a host group, such as (sc), to display the Hostgroup Information view for that host group. See *Hostgroup Information*, page 2-100.
Host	Hosts in the host group.
	Click a host name to display the Host Information view for that host. See *Host Information*, page 2-103.
	Click a host status-signal icon () to display the Service Detail view for all services running on that host. See *Service Detail*, page 2-26.
Services	Names of the services running on each host in the host group.
	Click a service name to display the Service Information view for that service. See *Service Information*, page 2-106.

Table 2-114: Links **To** the Status Grid View

Origin	Link
Status Summary, page 2-11	View Status Grid For All Host Groups
Host Detail, page 2-30	View Status Grid For All Host Groups
Host Problems, page 2-35	View Status Grid For All Host Groups
Status Overview, page 2-32	View Status Grid For All Host Groups
Service Detail, page 2-26, when main heading is Service Status Details For All Host Groups	View Status Grid For All Host Groups
Service Detail, page 2-26, for a single host group	View Status Grid For This Host Group

Table 2-114: Links **To** the Status Grid View (Continued)

Origin	Link
Hostgroup Information, page 2-100, for a single host group	View Status Grid For This Hostgroup
Status Grid view, for a single host group	View Status Grid For All Host Groups

Table 2-115: Links **From** the Status Grid View

Destination	Link
Host Detail, page 2-30	View Host Status Detail . . .
Service Detail, page 2-26	View Service Status Detail . . .
Status Overview, page 2-32	View Status Overview . . .
Status Summary, page 2-11	View Status Summary . . .
Status Grid view, for all host groups	View Status Grid For All Host Groups, when viewing Status Grid for a single host group.

MBean

The MBean view shows the operations (methods) and attributes exposed by a particular managed object (MBean, or JBoss component) for remote management purposes.

Note: *Do not modify* any settings in this view. For monitoring purposes, you normally do *not* need to use this view. It is intended for use only by installers and advanced system administrators.

To view the life-cycle state change history of an individual smart cell, click the link view the values of StateChangeHistory, found in the MBean view for the SmartCellStateControllerMBean of the smart cell:

View Cell Space view -> Agent view for the smart cell -> MBean view for the SmartCellStateControllerMBean -> Array view for StateChangeHistory

Related Views

- *View Cell Space*, page 2-24.

Table 2-116: Links **To** the MBean View

Origin	Link
Agent, page 2-111	any listed object
View Cell Space, page 2-24	Back to MBean View

Table 2-117: Links **From** the MBean View

Destination	Link
Agent, page 2-111	Back to Agent View
Array view (you normally do *not* need to use this view)	various

Agent

The Agent view shows the managed objects (MBeans, or JBoss components) currently running on a particular host machine.

Note: *Do not modify* any settings in this view. For monitoring purposes, you normally do *not* need to use this view. It is intended for use only by installers and advanced system administrators.

Noteworthy MBeans include the following –

- For smart cells:
  - ArchiveServiceMBean (document archiving)
  - Indexer (document indexing)
  - SmartCellStateControllerMBean
- For SMTP services:
  - SMTPService

Related Views

- *View Cell Space*, page 2-24.

Table 2-118: Links **To** the Agent View

Origin	Link
View Cell Space, page 2-24	• Back to Agent View • host name
MBean, page 2-110	Back to Agent View

Table 2-119: Links **From** the Agent View

Destination	Link
MBean, page 2-110	any listed object
Agent Administration view (you normally do *not* need to use this view)	Admin (button)

Smart Cell Groups for Domain

The Smart Cell Groups for Domain view provides performance information on each smart cell group in a domain.

Note: You will typically monitor this view daily.

The following table describes the information provided for a *single* smart cell group.

Table 2-120: Smart Cell Groups for Domain View Features, Single Group

Feature	Description
smart-cell group ID number	A smart-cell group identifier generated automatically by the RISS. This number is unique across all systems, everywhere.

Table 2-120: Smart Cell Groups for Domain View Features, Single Group

Feature	Description
Primary	IP address of the primary smart cell of the group. Additional primary smart cell information:
• State	• Current life cycle state of the smart cell – see *Smart Cell Life Cycle State Definitions*, page 1-4.
• Store Rate	• Number of documents currently being stored per second.
• Index Rate	• Number of documents currently being indexed per second.
• Archived	• Number of documents archived since smart cell was assigned.
• Indexed	• Number of documents indexed since smart cell was assigned.
• Docs Failed	• Number of documents that did not get indexed, since startup.
• Last Updated	• Date and time the smart cell was last updated.
Secondary	Secondary smart cell of the group. Same information as for the primary (see previous).
Replica	A remote replica of one or both smart cells in the group. Replicas are numbered 1 and 2. Same information as for the primary (see previous).
Graph	The document storage and indexing rates, and the difference between these rates, over the last 24 hours.

See Also

- *Detailed Email Reports*, page 2-47, for information on automatically sending email reports containing the same information as the Smart Cell Groups for Domain view.

Related Views

- *System Status*, page 2-14.
- Much of the information in the Smart Cell Groups for Domain view is also provided by the smart-cell information of the View Cell Space view (see *View Cell Space*, page 2-24).

Table 2-121: Links **To** the Smart Cell Groups For Domain View

Origin	Link
System Status, page 2-14	domain name (Smart Cell Group Information)

Table 2-122: Links **From** the Smart Cell Groups For Domain View

Destination	Link
System Status, page 2-14	Return to Summary

External Command Interface

You use the External Command Interface view to run a command that performs an action. Some commands allow or require you to enter additional command information. Fields labeled in red are required input. To run the command after entering any command information, click the Commit button. The Reset button clears (empties) all input fields.

The following table lists useful external commands. Some commands are applicable to individual hosts or services, or to all hosts of a host group or all services running on a host.

Table 2-123: External Commands

Shut down (stop) the Nagios process (PCC monitoring), so RISS is no longer monitored.
Restart the Nagios process (PCC monitoring).
Enable/disable sending notifications for hosts or services. See Example: Enabling/ Disabling Notifications, below.
Enable/disable checks (monitoring) of hosts or services.
Add a host or service comment. See Example: Adding a New Comment, below.
Schedule downtime for hosts or services
Schedule an immediate check of all services on a host.
Reschedule the next check of a service.

(Commands affecting passive checks, event handling, and flap detection are not useful; these features are *not used* by the PCC.)

Note: Commands that disable (notifications, status checks, and so on) override commands that enable. For example, suppose you

disable checks for a particular service such as PING using the Service Information view (command Disable checks of this service), but you enable checks for all services using the Nagios Info view (command Start executing service checks). The particular service (PING) is *not* checked, because disabling overrides enabling.

Example: Enabling/Disabling Notifications

If you click the Disabled button next to Notifications in the Tactical Overview view (see *Tactical Overview*, page 2-21), which indicates that notifications are currently disabled, the External Command Interface view appears with the message You are requesting to enable notifications. There is no additional command information to enter – just click the Commit button.

Example: Adding a New Comment

If you click the Add a new host (service) comment link in the Comments view (see *Comments*, page 2-36), the External Command Interface view appears with the message You are requesting to add a host (service) comment. Enter a host and service name, your name, and your comment. The Persistent check box is *not used*. (PCC comments are always persistent: they are not deleted when the Control Center shuts down.) Click Commit to execute the command.

Example: Acknowledging a Problem

You can use the Acknowledge this host/service problem command to let others know you have noticed a problem and are working on it. This command is available in the Host/Service Commands box of the Host/Service Information view whenever a host or service has a problem (see *Host Information*, page 2-103, and *Service Information*, page 2-106). You can remove a problem acknowledgement with the command Remove problem acknowledgement.

After you acknowledge a problem, problem notification for that host/service is disabled until it recovers. Contacts for the host/service receive notification of your acknowledgement (unless you turn off the Send Notification checkbox in the External Command Interface view when acknowledging).

Related Views

- *Application Manager*, page 2-76.
- *Tactical Overview*, page 2-21.

- *Comments*, page 2-36.
- *Nagios Info*, page 2-39.
- *Hostgroup Information*, page 2-100.
- *Host Information*, page 2-103.
- *Service Information*, page 2-106.

Table 2-124: Links **To** the External Command Interface View

Origin	Link
Tactical Overview, page 2-21	Enabled/Disabled
Comments, page 2-36	Add a new host/service comment
Downtime, page 2-37	Schedule host/service downtime
Nagios Info, page 2-39	commands (Process Commands)
Scheduling Queue, page 2-43	Actions for specific service
Hostgroup Information, page 2-100	commands (Hostgroup Commands)
Host Information, page 2-103	commands (Host Commands)
Service Information, page 2-106	commands (Service Commands)

Links *from* the External Command Interface view: none.

Updating and Printing Views

Update View Before Printing

PCC views displayed in your web browser are automatically updated every 90 seconds, approximately. To manually update the browser display at any time, click the Refresh (or Reload) button of your web browser.

If your browser caches web pages (most do), the cached view displayed after you use the browser Back button can be out of date. Refresh it manually.

Some browsers print from an updated version of the web page, without refreshing the browser display. This means that if the displayed view is out of date the printout can appear different from the view display. To be sure to print what you see displayed, refresh your browser manually before printing.

Print View Frame, Not Left Menu Frame or Entire HTML Page

The PCC web browser interface is an HTML (web) page composed of two HTML frames: the left frame contains the left menu; the right frame contains the current monitoring view. If you want to print the displayed view information, make sure that you print the view frame, not the left menu frame or the entire page (both frames). How to print a frame depends on what browser you use.

Microsoft Internet Explorer

Do either of the following to print a frame using the Microsoft® Internet Explorer® browser (version 6):

- Right-click anywhere in the view frame, then pick Print from the popup frame menu.
- Click anywhere in the view frame to make it active, then use the File menu Print or Print Preview command. If you use the Print Preview command (to check what will be printed), choose Only the selected frame in the rightmost pulldown menu.

Netscape Navigator

Do the following to print a frame using the Netscape Navigator® browser (version 7):

1. Right-click anywhere in the view frame, then pick This Frame -> Show Only This Frame from the popup frame menu. This shows only the view frame in the browser window (the left menu is not shown).
2. Use the File menu Print or Print Preview command.
3. Use the Back button to display the left menu again.

CHAPTER 3

Persist Account Manager

This chapter explains how to use the Persist Account Manager (PAM) to provision and update user accounts.

User Accounts and PAM

Persist Account Manager (**PAM**) is the tool you use to view and update individual user accounts for unusual circumstances on the HP StorageWorks Reference Information Storage System (RISS). The initial setup and routine addition and deletion of user accounts occurs automatically through synchronization with Windows Active Directory.

RISS archives email and other documents in one or more repositories. A **repository** is a virtual collection of documents associated with a given user by **routing rules** (for storing) and by **access control lists** (for retrieving). Users can find and retrieve archived documents to which they have access.

You use PAM to update user accounts as follows:

- add users that are not imported through dynamic account synchronization (DAS)
- add special-purpose repositories
- add or modify routing rules
- add users to new and existing access control lists

Note: You can view user accounts on replica domains, but PAM does not allow you to add or edit them. Fields cannot be edited and action buttons are unavailable when you select a domain that is a replica of another domain.

Installing PAM

PAM runs on Microsoft Windows platforms. To install PAM, just copy the `pam` directory from the Utilities CD to a Windows drive.

Logging into PAM

To log in to PAM, follow this procedure:

1. Navigate to the `pam/bin` directory on your Windows machine.
2. Double-click the filename `pam.bat`. The Login dialog box is displayed:

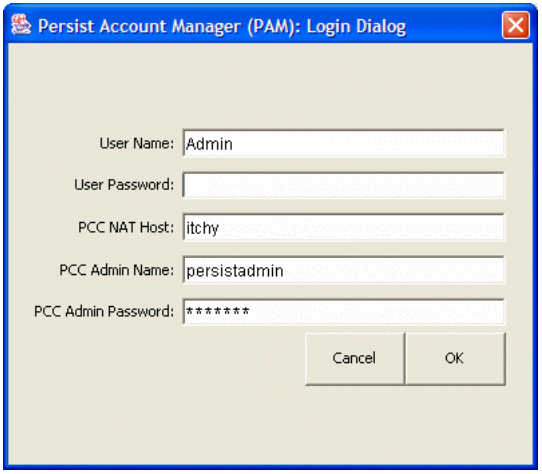


Figure 3-1: Persist Account Manager Login Dialog Box

3. Enter the following, and click OK. The Persist Account Manager window is then displayed (see *PAM Window*, on page 3-5).
   - User Name: Your user name. (You must be a user with administrative privileges to use PAM.)
   - User Password: Your password. This is empty (blank) initially. You can change your password using the RISS Web Interface (choose Preferences).
   - PCC NAT Host: The name or IP address of the PCC NAT host
   - PCC Admin Name: `persistadmin`
   - PCC Admin Password: password for accessing the Persist Control Center

PAM Window

After you log in to PAM (see *Logging into PAM, on page 3-4*), the Persist Account Manager window is displayed:

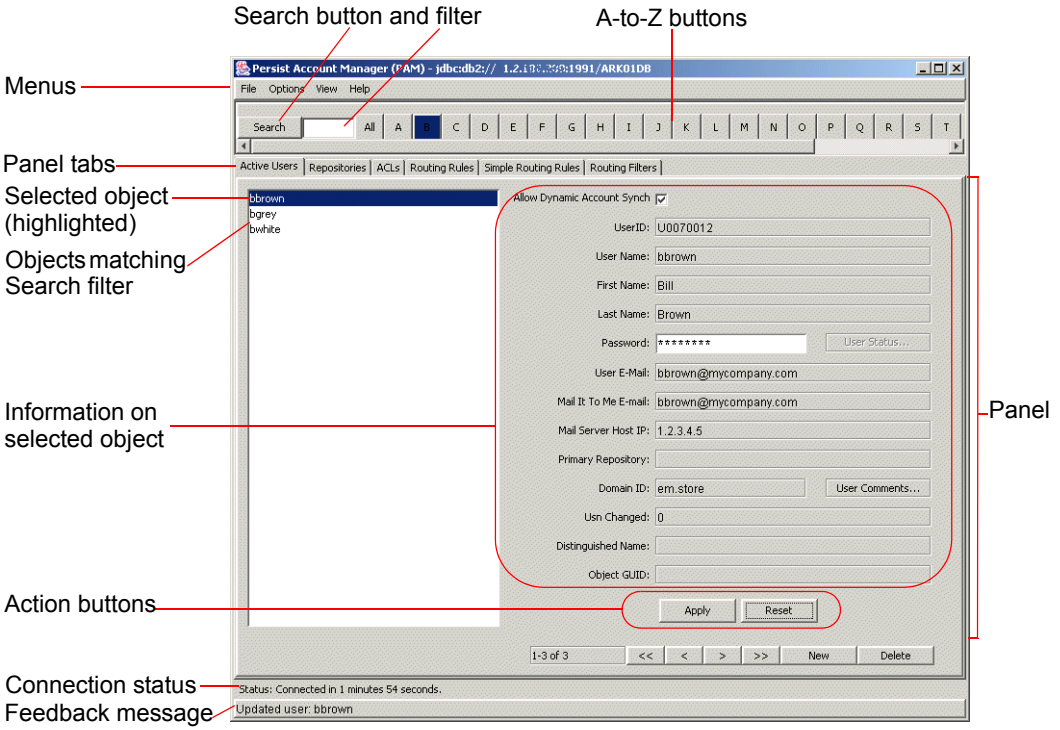


Figure 3-2: Persist Account Manager Window

The Persist Account Manager window has the following features:

Table 3-1: Persist Account Manager Window

Feature	Description
File menu	• Exit – Exits PAM.

Table 3-1: Persist Account Manager Window (Continued)

Feature	Description
Options menu	• Show Users – Determines which set of registered users is shown in the Users panel. Options are: – All Users – Shows all users of the system. – Active Users – Shows only users who are allowed to log in (active Outlook Integration Users and active Non-Outlook Integration Users). – Inactive Users – Shows only users who are not allowed to log in. – Outlook Integration Users – Shows only the active and inactive users of the Outlook Integration query system. – Non-Outlook Integration Users – Shows all users except Outlook Integration Users. – Admin Users – Shows only system administrator users. *Note:* The name of the Users panel reflects what you select (see *Users Panel, PAM Window*, on page 3-13). • Look and Feel – Determines the appearance of the PAM window. Choices are: Metal, Motif, and Windows.
View menu	Database Statistics – Displays the PAM Database Statistics Summary, which shows the number of users, repositories, ACLS, routing rules, and billing groups in the system.
Help menu	About – Shows the current version of PAM. PAM Help – Opens PAM online help in a browser window.
Search	Lists only the objects whose names start with the text you enter in the Search box. (Panels are described later in this table.) For example, in the Users panel you can search for ja to find users named jadams, jackdoe, and janedoe. Click the Search button to find matching objects. When the Domain box is present (see below), the search is limited to names in the selected domain.
Domain:	Determines the domain for which simple routing rules and filters are displayed. Select the domain from the pulldown list. The selection limits the scope of the Search and A-to-Z filter buttons. (Domain is available only when the current panel is Simple Routing Rules or Routing Filters.
All button	Lists all objects of the type indicated by the panel (tab) name.

Table 3-1: Persist Account Manager Window (Continued)

Feature	Description
A-to-Z buttons	Click a button to show only the names that start with the button letter. The names correspond to objects of the current panel. (Panels are described later in this table.) When the Domain box is present (see previous), names are limited to those in the selected domain. (These buttons are not available in the Routing Filters panel.)
scroll bar	Slide the scroll bar to bring the left or right end of the PAM window into view.
panels	Displays the objects depicted by the tab name. Click a tab to view the corresponding panel. All panels have these parts: • A list of (up to 50) objects corresponding to the tab name and filtered by the Search, Domain, and A-to-Z selections. • Information pertaining to the object that is selected in the list. • Apply button to save any changes you make to the displayed information. • Reset button to clear any changes you make (prior to clicking Apply) and redisplay the current database information. Individual panels display the following objects: • Users (see *Users Panel, PAM Window*, on page 3-13) – RISS users of the kind determined by Options > Show Users. Lets you create and delete users, view and edit user information, and change user status and privileges. • Repositories (see *Repositories Panel, PAM Window*, on page 3-16) – RISS repositories. Lets you create repositories and add, view, or delete repository access control lists. You cannot delete existing repositories. • ACLs (see *ACLs Panel, PAM Window*, on page 3-17) – Access control lists. Lets you create and delete ACLs and add or remove users to or from an existing ACL. • Routing Rules (see *Routing Rules Panel, PAM Window*, on page 3-19) – Lets you create, view, edit, and delete complex routing rules and associate them with repositories. • Simple Routing Rules (see *Simple Routing Rules Panel, PAM Window*, on page 3-21) – Lets you create, view, edit, and delete simple routing rules and associate them with repositories. • Routing Filters (see *Routing Filters Panel, PAM Window*, on page 3-23) – Lets you create, view, edit, and delete routing filters and associate them with repositories.

Table 3-1: Persist Account Manager Window (Continued)

Feature	Description
navigation buttons	Shows you which part of the total number of qualified objects is displayed, and lets you display other parts of the list. (For example, 1-50 of 230 means that the first fifty objects are shown and that a total of 230 objects match the selected type and filter criteria.) Click the navigation buttons to: • < – Display the previous 50 qualified objects. • << – Display the 50 qualified objects before the previous 50. • > – Display the next 50 qualified objects. • >> – Display the 50 qualified objects after the next 50. • New – Create a new object of the current panel type. This displays the Add New Item dialog box, which is specific to the current panel (see previous panel descriptions). • Delete – Delete the selected object.
connection status	Indicates how long it took PAM to connect to the database. Example: Status: Connected in 0 minutes 17 seconds.
feedback	Indicates the status of the last action. Example: Updated user: bbrown.

Using the PAM Window

Use the Persist Account Manager window to create, view, modify, or delete an object, such as a user account, ACL, or routing rule. This section explains how you do this in general.

To follow a sample scenario, see *Example: Integrating a New Department*, on page 3-26. For detailed information on individual PAM window panels, refer to the panel descriptions later in this chapter.

Creating PAM Objects

To create an object:

1. Click the New button to create the object. The Add New Item dialog box is displayed.
2. Define the object using the Add New Item dialog box.
3. Click Add.

Viewing, Modifying, and Deleting PAM Objects

To view, modify, or delete an object:

1. Click the tab that depicts the kind of object you want to view, modify, or delete. For example, click the Repositories, ACLS, or Routing Rules tab.
2. Use the Search, A-to-Z, <, <<, >, and >> buttons to display the target object in the list.
3. Select the target object in the list.
4. To modify the selected object, do one or more of the following, and then click the Apply button to save the changes.
   - Change the values in the editable parts of the panel.
   - If the selected object is a collection of other objects:

     Add or remove member objects to/from the collection, using the Add <*object type*> or Remove <*object type*> button, respectively. See *Adding/*

Removing Member Objects to/from a Collection Object, on page 3-10, for general addition and removal procedures.

(The following object types are **collections**: repositories, ACLs, simple routing rules, and routing filters.)

5. To delete the selected object, click the Delete button and then confirm deletion.

   Example: To delete an ACL, select it in the list and click Delete. Click Yes when the confirmation message appears.

Adding/Removing Member Objects to/from a Collection Object

This section describes the general procedures for adding objects to a collection and removing objects from a collection. These procedures assume you have first selected the collection object in the list at the left of the PAM window. See *Viewing, Modifying, and Deleting PAM Objects*, on page 3-9, for the context of the procedures described here.

To Add an Object to a Selected Collection Object

1. Click the Add <*type*> button to add an object of the indicated <*type*> to the selected collection object. (The particular object <*type*> depends on the current panel.)

   This displays the Select <*type*> dialog box. Here is the Select User dialog box, as an example:

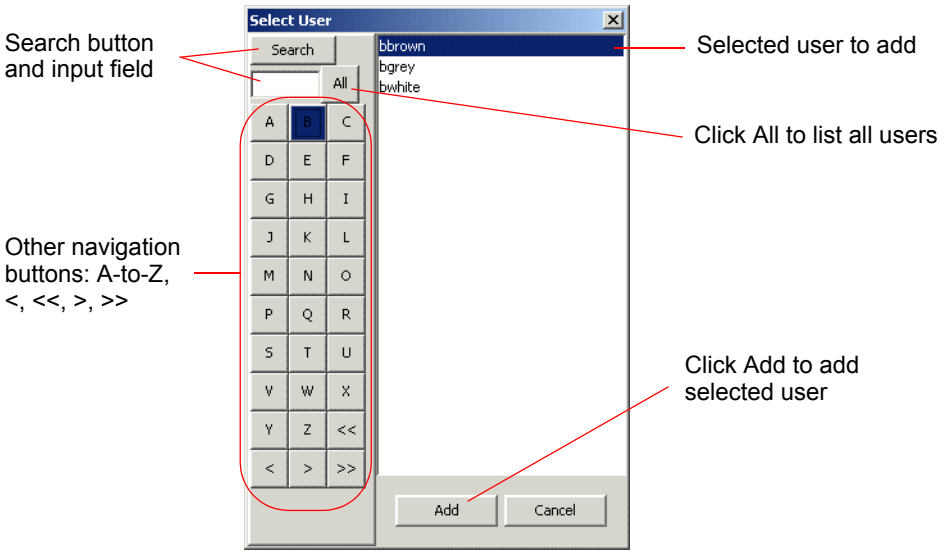


Figure 3-3: Select User Dialog Box

2. In the Select *<type>* dialog box, select the object you want to add to the collection. (Use the buttons Search, All, A-to-Z, or <, <<, >, and >> to navigate the list.)
3. Click the Add button in the Select *<type>* dialog box to add the selected object to the target collection object.
4. Click the Apply button in the PAM panel.

Example: To add a user to an access control list (ACL):

1. Select the ACL in the ACLs panel.
2. Click the Add User button.
3. Select the user to add in the Select User dialog box.
4. Click the Add button in the Select User dialog box.
5. Click the Apply button in the ACLs panel.

To Remove an Object from a Selected Collection Object

1. In the list of objects currently belonging to the selected collection object (at the right of the current panel), select the object you want to remove from the collection.
2. Click the Remove <*type*> button. (The particular object <*type*> depends on the current panel.)
3. Confirm removal (Yes) of the selected object.
4. Click the Apply button in the panel.

Example: To remove a user from an ACL:

1. Select the ACL in the list at the left of the ACLs panel.
2. Select the user to remove in the box User entries for this ACL.
3. Click the Remove User button in the ACLs panel, and confirm (Yes).
4. Click the Apply button in the ACLs panel.

Users Panel, PAM Window

Use the Users panel of the PAM window to view or change individual user accounts on RISS. You choose the set of users to view with the Options menu Show Users command – see *Options menu*, *Persist Account Manager Window*, on page 3-5. The panel name (on the tab) changes accordingly.

For example, if you choose Options -> Show Users -> Active Users, the panel heading is Active Users, and you can view only the active users (those able to log in to the system). If you, instead, choose Outlook Integration Users, the panel heading is Outlook Integration Users, and you can view only users that use RISS from within Microsoft Outlook.

Regardless of which set of users is selected by the panel, you can create or delete a user account, or change the privileges and identifying information for a given user.

The following table describes the features of the Users panel.

Table 3-2: Users Panel, PAM Window

Feature	Description
object list	Users on this system of the kind determined by the Options menu, Show Users command, and indicated by the current panel name. Only the first 50 items in the list are shown, and the list can be filtered using the Search and A-to-Z buttons. (See *Using the PAM Window*, on page 3-9.)
Synchronize this Account	Indicates whether or not DAS is allowed to update the selected user account. (See *User Manager*, on page 2-83, for information on DAS.) If selected, the User Name, First Name, Last Name, User E-Mail, Mail It To Me E-mail, Mail Server Host IP, and User Status fields cannot be edited. They are synchronized with values on the LDAP server.
UserID	Automatically generated identifier for the selected user; unique to the system. (Not editable.)
User Name	(Required.) System login name for the selected user.
First Name	First name of the selected user.
Last Name	Last name of the selected user.
Password	Login password for the selected user.

Table 3-2: Users Panel, PAM Window (Continued)

Feature	Description
User Status	Displays the following user profile options: • Active User – Selected if the user has a current login. • Outlook Initialized – Selected if the user uses RISS through Microsoft Outlook. • Administrative Privileges – Selected if the user is allowed to perform administrative tasks, such as using PCC and PAM. • BCC User – Selected if the user is allowed to view blind carbon copy addressees of the mail in the user's repositories. If you change the selected options, click Apply to save the changes. Otherwise, click Cancel to close the User Status dialog box. The User Status button is unavailable if Synchronize this Account is selected.
User E-Mail	Email address for the selected user.
Mail It To Me E-mail	(Required.) Email destination when the selected user clicks the Mail It To Me button for an archived document.
Mail Server Host IP	IP address of the mail server for the selected user. (Optional, unless querying within Microsoft Outlook is required.)
Primary Repository	The ID of the repository that was created with the selected user. (Not editable. Users can be given access to additional repositories through ACLs.)
Domain ID	Domain that the selected user belongs to. (Not editable. This value is supplied when the account is created.)
User Comments	Displays administrators' comments on the selected user account. Click User Comments to view the comment. In the Comment dialog box, click Update to add or change the comment. Type a new comment in the Input dialog box and click OK. The new comment replaces the previous comment. Click OK to close the Comment dialog.
Usn Changed	The USN imported from the corresponding user account on the LDAP server the last time DAS ran. (Not editable.) DAS uses this number to detect updates to the account (see page 2-83).
Distinguished Name	The corresponding object name, relative location in the LDAP tree, and domain. CN (Common Name) is the object name, cn is its branch in the tree, and dc values are the domain name. (Not editable.) DAS supplies this value.

Table 3-2: Users Panel, PAM Window (Continued)

Feature	Description
Object GUID	The Globally Unique Identifier of the corresponding user account on the LDAP server. (Not editable.) This is DAS' key to the correct account on the LDAP server.
Apply	Saves any changes that you make to editable fields. This button is unavailable until you change a value.
Reset	Clears any unsaved changes and redisplays the last saved values.
New button (specifics)	Lets you add a new user. Newly created users are automatically assigned active status, so they can log into the system. The Add New Item dialog box lets you choose the domain for the new user and enter name, email, and host information. You cannot select user status or enter comments. After you close the Add New Item dialog box, the Create User Options dialog box lets you choose either or both of the following options: • Add Repository, ACL & Simple Routing Rule – If selected (the default), a new individual repository is created for the user, together with a new ACL, giving the user access to the repository, and a new simple routing rule that routes all email to and from the user to the repository. The repository and ACL have the same name as the user. The user email address is also the name of the simple routing rule. • Add the following Complex Routing Rule – When enabled, a new complex routing rule is automatically created, defined by the text you enter in the accompanying field. See *Creating New Marketing Department Users*, on page 3-28, for an example of creating a user.

Repositories Panel, PAM Window

Use the Repositories panel of the PAM window to examine or change RISS repositories. You can add a new repository or change which ACLs apply to a given repository.

The following table describes the features of the Repositories panel.

Table 3-3: Repositories Panel, PAM Window

Feature	Description
object list	Repositories on this system. Only the first 50 items in the list are shown, and the list can be filtered using the Search and A-to-Z buttons. (See *Using the PAM Window*, on page 3-9.)
Repository ID	Automatically generated identifier for the selected repository. This number is unique to the system. (Not editable.)
Name	(Required.) Name of the selected repository.
Access ACL ID	ACLs defined for the selected repository. Double-click an ACL entry to display the ACL dialog box, where you can view (but not modify) the definition of that ACL. (The ACL dialog box provides the same information as the ACLs panel for that ACL – see *ACLs Panel, PAM Window*, on page 3-17.)
Domain Name	Domain that the selected repository belongs to. (This value is supplied when the repository is created. See *User Manager*, on page 2-83, for DAS configuration.)
Add ACLs	Click to display the Select ACL Entries dialog box, where you can select access control lists and add them to the selected repository. Click Apply in the Repositories panel for any addition to take effect.
Remove ACLs	Select an Access ACL ID entry, and then click Remove ACLs to remove that ACL from the selected repository. Click Apply for the removal to take effect.
Apply	Saves any changes that you make to editable fields. This button is unavailable until you change a value.
Reset	Clears any unsaved changes and redisplays the last saved values.
New button (specifics)	The Add New Item dialog box lets you define the repository name, choose its domain, and choose ACLs for the new repository. See *Creating a New Repository for the Marketing Department*, on page 3-29, for an example of creating a new repository.

ACLs Panel, PAM Window

You use the ACLs panel of the PAM window to create or delete an access control list, or to change the set of users in a given ACL.

The following table describes the features of the ACLs panel.

Table 3-4: ACLs Panel, PAM Window

Feature	Description
object list	Access control lists on this system. Only the first 50 items in the list are shown, and the list can be filtered using the Search and A-to-Z buttons. (See *Using the PAM Window*, on page 3-9.)
ACL ID	Automatically generated identifier for the selected ACL. This value is unique to the system. (Not editable.)
Name	(Required.) Name of the selected ACL. (Not editalbe. This value is supplied when the ACL is created. See *User Manager*, on page 2-83, for DAS information.)
Description	Description of the selected ACL. (Not editable here. This value is supplied when the ACL is created.)
User Entries for this ACL	List of user names in the selected ACL. Double-click an entry to display the User dialog box, where you can view (but not modify) the user profile. (The User dialog box provides the same information as the Users panel for that user – see *Users Panel, PAM Window*, on page 3-13.)
Add User	Click to display the Select User dialog box, where you can select and add one or more users to the selected ACL. Click Add in the Select User dialog box to add the selected user to the user entries in the ACLs panel. You must click Apply in the ACLs panel to implement the change. See *Adding/Removing Member Objects to/from a Collection Object*, on page 3-10, for an example.
Remove User	Select a user in the User Entries for this ACL list, and click Remove User to remove the selected user from the ACL. The user is not actually removed until you click Apply in the ACLS panel. See *Adding/Removing Member Objects to/from a Collection Object*, on page 3-10, for an example.
Apply	Saves any changes that you make to editable fields. This button is unavailable until you change a value.
Reset	Clears any unsaved changes and redisplays the last saved values.

Table 3-4: ACLs Panel, PAM Window (Continued)

Feature	Description
New button (specifics)	The Add New Item dialog box lets you define the ACL Name and Description, and choose the user entries for the new ACL. See *Creating a New ACL for Managers to Access Marketing Email*, on page 3-29, for an example of creating a new ACL.

Routing Rules Panel, PAM Window

You use the Routing Rules panel of the PAM window to create, edit, or delete a complex routing rule, or to choose the repository associated with a rule.

Note: Use simple routing rules (see *Simple Routing Rules Panel, PAM Window*, on page 3-21), instead of the Routing Rules panel, whenever possible. Extensive use of complex rules can negatively impact system performance.

The following table describes the features of the Routing Rules panel.

Table 3-5: Routing Rules Panel, PAM Window

Feature	Description
candidate objects	List of all complex routing rules. Only the first 50 items in the list are shown, and the list can be filtered using the Search and A-to-Z buttons. (See *Using the PAM Window*, on page 3-9.)
Routing Rule ID	Automatically generated identifier for the selected routing rule. This value is unique to the system. (Not editable.)
Name	(Required.) Name of the selected routing rule.
Domain	Domain of the selected routing rule. (Not editable here. This value is supplied when you create the rule, using the New button.)
Repository	Repository the routing rule applies to. Emails that match the rule are routed to this Repository.
. . .	Click the . . . (ellipsis) button to display the Select Repository dialog box, where you choose the destination repository.

Table 3-5: Routing Rules Panel, PAM Window (Continued)

Feature	Description
Routing Rule Info	Definition of the routing rule. *Note:* Matching is *not* case-sensitive (b matches both B and b), with the exception of the Subject field. *Syntax:* • Each match string is composed of ISO 8859-1 (Latin-1) characters enclosed in double quotes ("). • Each match component includes a keyword followed by an equals sign (=) and a match string. Example: TO="w@z.org". • Keywords for match components: – A TO component matches any email recipient field (To, Cc, Bcc, Apparently-To). – A FROM component matches the email sender field (From). – A Subject component matches any string in the email Subject field. Example: Subject="meeting" matches Subject: What time is today's Meeting?. Matching of the Subject field is case-sensitive: (b matches b, but not B; B matches B, but not b). – A MessageDateRange component checks when an email was *sent*; it matches if the email Date field is within the indicated range. The match string is "<*date1*> TO <*date2*>", where each date has the syntax of an email Date field (date, local time, local offset from GMT). Example: MessageDateRange="2003-7-1 00:00 +0700 TO 2003-8-1 00:00 +0700". • Email addresses are used as match strings for TO and FROM. Each must respect the standard email address syntax. Each is matched completely; for example, TO="c@b.com" matches c@b.com, but *not* abc@b.com. • Parentheses ((,)) are used for grouping. Example: (FROM="a@b.com" OR (TO="w@z.org" AND Subject="meeting")).
New button (specifics)	The Add New Item dialog box lets you define the rule Name, choose the domain and the repositories for the new routing rule, and define the Routing Rule Info.

Simple Routing Rules Panel, PAM Window

You use the Simple Routing Rules panel of the PAM window to create, edit, or delete a simple routing rule, or to choose the repository associated with a rule.

Note: Use simple routing rules, instead of the Routing Rules panel (see *Routing Rules Panel, PAM Window*, on page 3-19), whenever possible. Extensive use of complex rules can negatively impact system performance.

The following table describes the features of the Simple Routing Rules panel.

Table 3-6: Simple Routing Rules Panel, PAM Window

Feature	Description
candidate objects	List of all simple routing rules for a selected domain. Only the first 50 items in the list are shown, and the list can be filtered using the Search and A-to-Z buttons. (See *Using the PAM Window*, on page 3-9.
Mail Address	(Required.) Mailing address of the selected simple routing rule. (Not editable here. You supply this value ith the New button.) The Mail Address is matched against both sender and recipient addresses. (It corresponds to Routing Rule Info (TO= . . . OR FROM= . . .) for a complex routing rule – see *Routing Rules Panel, PAM Window*, on page 3-19.)
Repository ID	(Required.) List of the repositories this simple routing rule applies to. Emails that match the rule are routed to each of these repositories. Double-click a repository ID to display the Repository dialog box, where you can view (but not modify) the definition of that repository. (The Repository dialog box provides the same information as the Repositories panel for that repository – see *Repositories Panel, PAM Window*, on page 3-16.)
Add Rep	Click to display the Select Repository dialog box, where you add one or more repositories to the selected simple routing rule. You must click Apply in the Simple Routing Rules panel before the addition takes effect. See *Editing Simple Routing Rules for Marketing Email*, on page 3-30, for an example of adding a repository to a simple routing rule.

Table 3-6: Simple Routing Rules Panel, PAM Window (Continued)

Feature	Description
Remove Reps	Select a repository in the Repository ID list, and click Remove Reps to remove the selected repository from the list. The repository is not removed from the routing rule until you click Apply in the Simple Routing Rules panel.
New button (specifics)	The Add New Item dialog box lets you define the Mail Address and choose the applicable repositories. *Note:* For a simple routing rule to have any effect, there must be a routing filter with the same email domain as in the routing rule Mail Address. When you create a new simple routing rule, make sure you check the Routing Filters panel for a filter with the corresponding domain. If there is no such filter, create one. See *Routing Filters Panel, PAM Window*, on page 3-23.

Routing Filters Panel, PAM Window

You use the Routing Filters panel of the PAM window to create, edit, or delete a routing filter, or to choose the repositories associated with a routing filter.

A **routing filter** checks the email domains that appear in all of the addresses of each email. For each domain in an email that matches the Email Domain of a routing filter, both of the following occur:

- All simple routing rules with that domain are checked against the email. The simple routing rules that match the email are then applied (routing the email to the repositories associated with the rules).
- The email is routed to the repository (Repository ID) defined for the filter—provided the Repository ID of the filter does *not* include the special value R0000000 Catchall Repository.

This means that a routing filter has two possible uses, both based on which domains appear in email addresses:

- It filters emails before simple routing rules try to match them: only the rules with the right email domains are tried.
- It routes emails from a specific domain to a specific repository. (In this case, it is typically used to associate an audit repository with an email domain.)

After filtering, each email is always checked against complex routing rules. This is so regardless of the result of filtering (possible routing by simple rules and/or filter).

R0000000 Catchall Repository

The special value R0000000 Catchall Repository is an exception. A filter with this value in the Repository ID does *not* route email to the catch-all repository. It does *not*, itself, route mail to any repository; rather, it serves only as a filter before checking simple routing rules.

You can create a routing filter with the special value R0000000 Catchall Repository by choosing Catchall Repository in the Select Repository dialog box – see below. Do this when you want only to filter email before checking simple routing rules, without also routing email directly to a repository based on the email domain.

Note: Before you add a repository to a filter Repository ID field that already contains the special value R0000000 Catchall Repository, *y*ou must first remove the entry R0000000 Catchall Repository. A routing filter with R0000000 Catchall Repository must *not* contain any other Repository ID values.

Routing Filter Examples

The following table shows what happens when emails with various addresses are filtered using different values for Repository ID. The Email Domain of each filter is the same in all the examples: ourcorp.com. (Each example shows a single email, with multiple addresses.)

Table 3-7: Routing Filter Examples

Repository ID	Addresses In the Email	Actions
marketingstore	johndoe@ourcorp.com, janechoi@ourcorp.com, june@other.com	• Check for simple routing rules matching johndoe@ourcorp.com and janechoi@ourcorp.com. • Route email to marketingstore. • Check for matching complex routing rules.
R0000000 Catchall Repository	johndoe@ourcorp.com, janechoi@ourcorp.com, june@other.com	• Check for simple routing rules matching johndoe@ourcorp.com and janechoi@ourcorp.com. • Check for matching complex routing rules.
<any>	june@other.com, johndoe@another.com	Check for matching complex routing rules.

The following table describes the features of the Routing Filters panel.

Table 3-8: Routing Filters Panel, PAM Window

Feature	Description
candidate objects	List of routing filters for a selected domain. Only the first 50 items in the list are shown.

Table 3-8: Routing Filters Panel, PAM Window (Continued)

Feature	Description
Email Domain	(Required.) Email domain of the selected routing filter (example: mycorp.com). The filter applies to all emails with this domain in the mail header. (Not editable. This value is supplied when the fiilter is created.)
Repository ID	(Required.) The repository that emails from the Email Domain are routed to (in addition to users' repositories) unless the R0000000 Catchall Repository is specified – see *Note*, above.
. . .	Click the . . . (ellipsis) button to display the Select Repository dialog box, where you can add a repository to the selected routing filter. The new repository replaces the previous repository in the Routing Filters panel. You must click Apply in the Routing Filters panel for the addition to take effect. Before adding a repository, make sure R0000000 Catchall Repository is *not* a Repository ID – see *Note*, above.
Apply	Saves any changes that you make to editable fields. This button is unavailable until you change a value.
Reset	Clears any unsaved changes and redisplays the last saved values.
New button (specifics)	The Add New Item dialog box lets you define the Email Domain, choose the domain of application for the new routing filter, and choose the applicable repositories.

See Also

- *Simple Routing Rules Panel, PAM Window*, on page 3-21.
- *Routing Rules Panel, PAM Window*, on page 3-19, for information on complex routing rules.

Example: Integrating a New Department

Problem Statement and Solution

Problem

In this example scenario, your company, OurCorp, is splitting off its marketing function from the Sales Department, to create a separate Marketing Department. The current marketing person, Mark Marcom, is becoming the manager of the Marketing Department, and two new marketing employees, John Doe and Jane Choi, are being hired.

You need to integrate the new Marketing department into the RISS archiving and retrieval system.

Solution

One way to accomplish this is as follows:

1. Create a single repository, marketingstore, for all email to and from Marketing Department personnel (John, Jane, and Mark). Use the Repositories panel to do this. See *Creating a New Repository for the Marketing Department*, on page 3-29, for a description of this task.

2. Create an ACL to access (query) the marketingstore repository. Only Mark, the Marketing Department manager, and Betty Bigboss, the company CEO, will belong to this ACL, since it will enable them to see all email to and from John, Jane, and Mark. Use the ACLs panel to do this. See *Creating a New ACL for Managers to Access Marketing Email*, on page 3-29, for a description of this task.

   Because you need to select one or more existing ACLs when you create a repository, you need to create the marketing ACL before the repository.

3. Create users johndoe and janechoi for the new employees John and Jane. Use the Users panel to do this. See *Creating New Marketing Department Users*, on page 3-28, for a description of this task.

   Creating these users will also automatically accomplish all of the following (provided the option ACL & Simple Routing Rule is enabled in the Create User Options dialog box – the default value):

- Create individual repositories for John's email and Jane's email.
- Create access control lists (ACLs) for John and Jane to access (query) their respective individual repositories.
- Create simple routing rules to route John's and Jane's email to their respective individual repositories.

The new repositories and ACLs are named the same as the users (johndoe and janechoi). The new simple routing rules are named with the user email addresses (johndoe@ourcorp.com and janechoi@ourcorp.com).

4. Edit the simple routing rules for the members of the Marketing Department (Mark, John, and Jane), to route their individual incoming and outgoing email to the marketingstore repository (in addition to routing it to their own repositories). Use the Simple Routing Rules panel to do this. See *Editing Simple Routing Rules for Marketing Email*, on page 3-30, for a description of this task.

See Also

- *Users Panel, PAM Window*, on page 3-13
- *Repositories Panel, PAM Window*, on page 3-16
- *ACLs Panel, PAM Window*, on page 3-17
- *Simple Routing Rules Panel, PAM Window*, on page 3-21

Alternative Solutions

There are of course alternative ways to satisfy the needs of adding a new department and new users, with the appropriate email routing and query access. For example, instead of creating a separate marketing ACL for the marketing repository, you could add the individual manager ACLs (Mark's and Betty's) to the marketing repository. Or you could dispense with both marketing ACL and marketing repository, by adding Mark and Betty to the ACLs for John's and Jane's individual repositories.

The relations between users, repositories, ACLs, and simple routing rules are all *N*-to-*M*: any number of users can be associated with any number of repositories, and so on. The way you organize these different entities and relations is up to you, but consistency is usually rewarded. Choose a scheme and stick to it.

For ease in maintenance and flexibility in access control, using abstract collection objects like a marketing repository and a marketing ACL can be advantageous. Trying, instead, to manage everything at the fine-grain level of individual users and their relations to user repositories can lead to extra work for both system administrators and end users.

For example, with a Marketing Department repository, a manager can limit a query to search only Marketing Department email.

Creating New Marketing Department Users

Use the Users panel to create new, active users for John and Jane. (It does not matter which kind of users are currently displayed in the Users panel.) Do the following once for John and once for Jane.

1. Click the tab of the Users panel to show the panel.
2. Click the New button. This displays the Add New Item dialog box, where you define the new user.
3. Enter the following to define the new user:
   - User Name – for John it is johndoe; for Jane it is janechoi.
   - First Name (John; Jane) and Last Name (Doe; Choi)
   - Leave the Password blank (empty). John and Jane will set their own passwords after they log in to the query system.
   - User E-Mail and Mail It To Me E-Mail – johndoe@ourcorp.com and janechoi@ourcorp.com (use the same addresses for each field).
   - Mail Server Host IP – the mail server IP for the company Ourcorp is 192.68.10.3.
   - Domain ID – choose the email domain ourcorp.com from the pulldown list of existing domains for your company.
4. Click Add to create the new user. The Create User Options dialog box is displayed – just click OK, without changing the default option values.

   When enabled (the default), the option ACL & Simple Routing Rule automatically creates a new repository, ACL, and simple routing rule for the new user. This gives the user access to his/her own repository, where all of his/her incoming and outgoing email is routed.

5. Click Apply in the Users panel (PAM window) to commit your changes to the database.

Creating a New ACL for Managers to Access Marketing Email

Use the ACLs panel to give Manager Mark and CEO Betty access to all email to and from members of the Marketing Department. Do the following:

1. Click the tab of the ACLs panel to show the panel.
2. Click the New button. This displays the Add New Item dialog box, where you define the new access control list for the Marketing Department.
3. Enter the following to define the new ACL:
   - Name – marketingaccess.
   - Description – Access to the Marketing Department repository.
   - User entries for this ACL – Click Add User. Use the Select User dialog box to choose the users to add to the new ACL: markmarcom and bettybigboss. Click Add in the Select User dialog box to finish adding to the ACL.
4. Click Add in the Add New Item dialog box to create the new ACL.
5. Click Apply in the ACLs panel (PAM window) to commit your changes to the database.

Creating a New Repository for the Marketing Department

Use the Repositories panel to create a new repository, marketingstore, for the marketing department. Do the following.

1. Click the tab of the Repositories panel to show the panel.
2. Click the New button. This displays the Add New Item dialog box, where you define the new individual user repository.
3. Enter the following to define the new Marketing Department repository:
   - Name – marketingstore.
   - Access ACL ID – Click Add ACL. Use the Select ACL Entries dialog box to choose the ACL to add to the new repository: marketingaccess. Click Add

in the Select ACL Entries dialog box to finish adding ACLs to the repository.

4. Click Add in the Add New Item dialog box to create the new repository.
5. Click Apply in the Repositories panel (PAM window) to commit your changes to the database.

Editing Simple Routing Rules for Marketing Email

Use the Simple Routing Rules panel to add the new Marketing Department repository, marketingstore, to the existing simple routing rules for each of the Marketing Department users (John, Jane, and Mark):

1. Click the tab of the Simple Routing Rules panel to show the panel.
2. Use the A-to-Z buttons or Search button to navigate to the list of candidate objects that contains the user email address.
3. Select the email address of the user in the list of candidate objects.
4. Click Add Rep. Use the Select Repository dialog box to add the marketingstore repository to the simple routing rule for the user, so email to and from the user will also be routed to the Marketing Department repository. Click Add in the Select Repository dialog box.
5. Click Apply in the Simple Routing Rules panel (PAM window) to commit your changes to the database.

INDEX

E

F

H

I

L

M

N

O

P

Q

R

S

U

V

W